



Airpower Lessons for an Air Force Cyber-Power Targeting Theory

Steven J. Anderson
Lieutenant Colonel, USAF



Air University

Steven L. Kwast, Lieutenant General, Commander and President

School of Advanced Air and Space Studies

Thomas D. McCarthy, Colonel, Commandant and Dean

AIR UNIVERSITY
SCHOOL OF ADVANCED AIR AND SPACE STUDIES



**Airpower Lessons for an Air Force
Cyber-Power Targeting Theory**

STEVEN J. ANDERSON
Lieutenant Colonel, USAF

Drew Paper No. 23

Air University Press
Air Force Research Institute
Maxwell Air Force Base, Alabama

Project Editor
Belinda L. Bazinet

Copy Editor
Carolyn J. Burns

Cover Art, Book Design, and Illustrations
Daniel Armstrong

Composition and Prepress Production
Nedra O. Looney

Print Preparation and Distribution
Diane Clark

AIR FORCE RESEARCH INSTITUTE

AIR UNIVERSITY PRESS

Director and Publisher
Dale L. Hayden, PhD

Editor in Chief
Oreste M. Johnson

Managing Editor
Dr. Ernest Allan Rockwell

Design and Production Manager
Cheryl King

Air University Press
600 Chennault Circle, Bldg. 1405
Maxwell AFB, AL 36112-6010
afri.aupress@us.af.mil

<http://aupress.au.af.mil>
<http://afri.au.af.mil/>

AFRI **AU PRESS**
AIR FORCE RESEARCH INSTITUTE

Library of Congress Cataloging-in-Publication Data

Names: Anderson, Steven J., 1970- author.
Title: Airpower lessons for an Air Force : cyber-power targeting theory / Steven J. Anderson.
Description: Maxwell Air Force Base, Alabama : Air University Press, Air Force Research Institute, [2016] | Series: Drew paper, ISSN 1941-3785 ; no. 23 | Includes bibliographical references.
Identifiers: LCCN 2016003567 | ISBN 9781585662388
Subjects: LCSH: Cyberspace operations (Military science)—United States. | United States. Air Force. | Military doctrine—United States. | Airpower—United States—Case studies.

Classification: LCC U163 .A62 2016 | DDC 358.4/14—dc23 LC record available at <http://lccn.loc.gov/2016003567>

Published by Air University Press in September 2016

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the School of Advanced Air and Space Studies, the Air Force Research Institute, Air University, the United States Air Force, the Department of Defense, or any other US government agency.

This publication is cleared for public release and unlimited distribution. This Drew Paper and others in the series are available electronically at the AU Press website: <http://aupress.au.af.mil>.

The Drew Papers

The Drew Papers are award-winning master's theses selected for publication by the School of Advanced Air and Space Studies (SAASS), Maxwell AFB, Alabama. This series of papers commemorates the distinguished career of Col Dennis "Denny" Drew, USAF, retired. In 30 years at Air University, Colonel Drew served on the Air Command and Staff College faculty, directed the Airpower Research Institute, and served as dean, associate dean, and professor of military strategy at SAASS. Colonel Drew is one of the Air Force's most extensively published authors and an international speaker in high demand. He has lectured to over 100,000 students at Air University as well as to foreign military audiences. In 1985 he received the Muir S. Fairchild Award for outstanding contributions to Air University. In 2003 Queen Beatrix of the Netherlands made him a Knight in the Order of Orange-Nassau for his contributions to education in the Royal Netherlands Air Force.

The Drew Papers are dedicated to promoting the understanding of air and space power theory and application. These studies are published by the Air University Press and broadly distributed throughout the US Air Force, the Department of Defense, and other governmental organizations, as well as to leading scholars, selected institutions of higher learning, public-policy institutes, and the media.

Please send inquiries or comments to

Commandant and Dean
School of Advanced Air and Space Studies
125 Chennault Circle
Maxwell AFB, AL 36112
Tel: (334) 953-5155
DSN: 493-5155
saass.admin@us.af.mil

Contents

List of Illustrations	<i>vii</i>
Foreword, Col John A. Warden III, USAF, retired	<i>ix</i>
Foreword, Col M. V. Smith, USAF	<i>xi</i>
About the Author	<i>xiii</i>
Acknowledgements	<i>xv</i>
Abstract	<i>xvii</i>
1 Introduction	1
2 From Airpower Development to Targeting the Industrial Web	17
3 Targeting: From Industrial Web to Warden's Rings	37
4 Artifacts for Cyber Power Targeting	61
5 Hypothesizing a Cyber-Power Targeting Theory	87
6 Conclusion	131
Abbreviations	135
Bibliography	137

Illustrations

Table

2.1	AWPD 42 target priorities	28
2.2	AWPD 42 target systems	28
2.3	Early airpower theorists and target objectives	32
3.1	JCS four-phase air campaign proposal	41
3.2	JCS 94-target scheme	41
3.3	Warden's five-ring model with objectives	45
3.4	Initial Gulf War objectives	51
3.5	Airpower theorists and target objectives	56
4.1	US cyber authorities and current title responsibilities	73
4.2	1991 Gulf War: centers of gravity and critical vulnerabilities	78
5.1	Principles of war	92
5.2	Ten propositions regarding cyberspace operations	94

Figure

3.1	Warden's five rings	46
3.2	Warden's updated rings	48
5.1	Military phases of operation	108

Foreword

Throughout the history of warfare, new weapons and techniques have appeared with great frequency. Most of them have emerged incrementally, taking many years from first introduction to widespread use and impact. Roughly until the advent of the twentieth century, they all functioned in the dimensional world of the land or sea. Then, for the first time, man ventured into the third dimension above and below the earth's surface. These genuinely disruptive ventures into a new dimension radically changed warfare in a remarkably short period of time.

Almost simultaneously, wireless transmission of information appeared. While wireless operated in a spectrum previously unknown, its primary impact on war operations was to improve communications. Although very important, it was not disruptive in the same way as airpower. Now, as we move into the twenty-first century, wireless has morphed into the cyber realm—the realm of bits and bytes traveling through multiple conduits to affect in peace, and presumably in war, nearly every facet of our lives. The speed of the movement into the cyber world has been breathtaking, as has been the almost daily introduction of new cyber tools and techniques unimaginable even a few years ago. Like airpower, cyber now adds a new, unexplored, and disruptive dimension to warfare. If we accept the possibility or, more likely, the probability of cyber warfare, we must recognize that we are in *terra incognita* with little to guide us.

Most inventions, even those that become truly disruptive, initially serve only to provide a marginally better way to accomplish something; it often takes decades before it becomes clear that these inventions enable entirely new concepts of operation never previously conceived. So it was with airpower, and so to date in the civilian world has it been in the cyber world. We don't know, but can guess, that cyber will have disruptive possibilities in war and that those who grasp the possibilities may well have huge advantages over those lingering in the past. What is the solution?


Lt Col Steven J. Anderson has made a significant step forward by providing a methodology to come to grips with the intriguing world of cyber—a world that offers great advantages in war to those who understand it and poses great, perhaps fatal, dangers to those who do not. His work is not a handbook of technology, but a philosophical guide to thinking through a very challenging problem—how to be prepared for cyber war. As the reader will see, he has built on a century of experience in the development of airpower to help find the answers. As suggested in his title, he has put “targeting” at the center of his efforts.

If we think about any competitive enterprise—business or war—two key elements of strategy are always (1) what is to be accomplished that will constitute success (objectives)? and (2) against what do resources need to be

committed to create the required system change that will lead to success? At the most basic level, the latter are targets. What needs to be hit or otherwise affected? Although the idea of objectives and targets as primary elements of strategy seems so simple, in the real world, targets are rarely given the attention they deserve.

Practitioners of both business and war have a tendency to leap from objectives, often poorly conceived and unclearly stated, to tactics—the means of business or war. As an example, early airpower practitioners, and even many today, pay only lip service to objectives, immediately leaping to employment of their technology to do something, anything, with little regard for the targets actually needed to achieve objectives. Taking this course puts the emphasis on activity and the tools of the trade, not on what is to be accomplished and why. Colonel Anderson has convincingly demonstrated the extraordinary importance of identifying the targets before becoming consumed with the tools or the doctrine of their employment. If you know what must be affected, either offensively or defensively, you have a clear path to think through the tools you need (*equip*); you can assemble the pieces (*organize*); and you can prepare to employ (*train*). Very simply, Colonel Anderson has given us a methodology to ensure that we become as prepared as we can to engage in something never before attempted on a military scale.

I am personally very pleased to have had the opportunity to share a few ideas with Colonel Anderson and have been quite impressed with how he has incorporated them into a much larger whole. In addition, he has drawn on a wide range of expertise and presented it all in a compelling thesis. One only hopes that the right people in the right places read what he has written.


JOHN A. WARDEN III
Colonel, USAF, Retired

Foreword

What Lt Col Steven “Canyon” Anderson has achieved with this work is nothing short of remarkable. While other authors provide little more than articulation of the problems introduced by cyber power, Canyon lays out a cogent road map for the Air Force to succeed in this new medium. By hearkening back to the origins of airpower theory and doctrine and tracing their evolution forward, he reveals how elements of cyber power fit within traditional Air Force roles and missions.

Canyon does not suggest that cyber power is exclusively an Air Force function. On the contrary, he goes to great lengths to explain that the Air Force should have no more than a limited set of cyber roles and missions to do its part in a much larger joint, multiagency national cyber effort. In fact, this work could be used as a handbook for those who wrestle with assigning cyber roles and missions to both the Unified Command Plan and the *Quadrennial Defense Review*.

In constructing his argument, Canyon introduces his readers to the first airpower theorists, such as H. G. Wells, who wrote prolifically about airpower’s utility and application in war—long before the Wright brothers’ fateful first flight at Kitty Hawk. He moves the story through World War I and the interwar years, showing how airmen incrementally advanced the art of airpower. In essence it boiled down to targeting strategy—what to strike—and an acquisition strategy to acquire the tools to hold identified target sets at risk. His description of the industrial web theory developed by the airmen of the Air Corps Tactical School on the eve of World War II, and its mixed success during the war, illustrates the requirement for theory, doctrine, and technology to keep pace with one another—a demand with which contemporary cyber power continues to struggle.

At the heart of Canyon’s research are extensive interviews and discussions with Col John Warden, the creator of the famous five rings model for airpower targeting. Working together, Anderson and Warden adjusted the five rings model to accommodate specific cyber power applications within current airpower roles and missions. The resulting construct does not limit cyber power applications to a mere augmentation of airpower, nor does it limit it to destructive means. Rather, it clarifies both the independent and combined-arms roles of the full spectrum of cyber power, as it should be employed.

This work represents the first cyber power theory tailored to a single-service community. It should, however, be read by every cyber professional, not just those in the Air Force. Colonel Anderson’s thesis received the Air University Foundation’s 2013 award for the best School of Advanced Air and Space Studies

(SAASS) thesis dealing with issues of technology, space, or cyberspace. In the finest tradition of literature produced by SAASS students, Canyon's masterpiece captures the essence of the school's motto From the Past, the Future!

A handwritten signature in black ink that reads "M. V. 'Coyote' Smith". The signature is stylized with a large, sweeping loop at the end. Above the first part of the signature is a small five-pointed star. Below the middle part of the signature is a small, simple cartoon drawing of a character with a round head and a small body.

M. V. "COYOTE" SMITH, Colonel, PhD
Professor of Strategic Space and Cyber Studies
School of Advanced Air and Space Studies

About the Author

Lt Col Steven Anderson received his commission in April 1999 through the Officer Training School at Maxwell AFB, Alabama. He is a cyberspace operator for the US Air Force (USAF). His first commissioned assignment was at Robins AFB, Georgia, where he performed combat airfield and combat support operations as a maintenance control officer and flight commander. He then moved to Incirlik Air Base, Turkey, where he was a support flight commander, group executive officer, and wing executive officer. Next, Colonel Anderson attended the US Marine Corps Expeditionary Warfare School at Marine Corps Base Quantico, Virginia, followed by a two-year Pentagon tour as an Air Force intern. Upon leaving Washington, DC, he deployed for a year as the deputy commander, 380th Expeditionary Communications Squadron, in the United Arab Emirates. Following this tour, he performed officer assignment and force development duties related to cyber operations at the Air Force Personnel Center, Randolph AFB, Texas. In August 2009 Colonel Anderson assumed the duties of executive officer for the newly established Twenty-Fourth Air Force at Lackland AFB, Texas. Next, in June 2010, he served as commander of the 3rd Combat Communications Support Squadron at Tinker AFB, Oklahoma—where he remained until his assignment to the School of Advanced Air and Space Studies (SAASS) in June 2012.

Colonel Anderson has a bachelor of arts degree in management, computer information systems, from Parkville University, Missouri, a master of business administration degree from Webster University, Missouri, and a master of arts degree in organizational leadership from the George Washington University in Washington, DC. Following graduation from SAASS, he reported for duty at US Pacific Command/J6 staff. Colonel Anderson is blessed to be married to his wife and has three beautiful children.

Acknowledgments

This work would not have been possible without the support of many truly remarkable people. I would like to offer my sincere appreciation to the faculty and staff at the School of Advanced Air and Space Studies. This is an extraordinary academic institution, and I am blessed to have been a part of it. In particular, I would like to thank my advisor, Col Michael “Coyote” Smith. His guidance and insight helped shape the final product in many invaluable ways. I would also like to thank Lt Col Richard Bailey for his perspective and critique of this work. Additional faculty at SAASS whom I would like to thank for supporting this thesis include Dr. Richard Muller, Dr. James Forsyth, Dr. Hal Winton, Dr. Stephen Wright, Col Suzanne Buono, and Lt Col David Woodworth. To my fellow classmates in Class XXII, thanks for making it a great year! I am humbled to have been included in such an outstanding group of leaders, officers, professionals, and strategists.

I would like to personally thank the many individuals who assisted in research or guidance toward subject material in support of this work. I apologize up front if I inadvertently left someone unrecognized. It was not intentional. In no particular order, I would like to thank Maj Gen Suzanne Vautrinot, USAF, retired; Brig Gen Bradford Shwedo (Air Combat Command/A2); Brig Gen Robert Skinner (Air Forces Cyber/Inspector General); Col Paul Welch (Twenty-Fourth Air Force); Col Thomas McCarthy (director, Center for Strategy and Technology); Dr. Kamal Jabbour (Air Force Research Laboratory/Information Directorate); Dr. Richard Raines (Air Force Institute of Technology [AFIT]/Department of Electrical and Computer Engineering); Dr. Robert Mills (AFIT/Department of Electrical and Computer Engineering); Lt Col Aldwin Estrellado (AF/A3CF/A6CF); Lt Col Leonard Pilhofer, USAF, retired; Lt Col Michael Birdwell (91st Network Warfare Squadron); Lt Col Christian Basballe Sorensen (US Cyber Command); Lt Col Steven “Kuna” Lindquist (328 Weapons School/DO); Lt Col Scott Vickery (26th Operations Support Squadron); Mr. Brian MacDougald (26th Operations Support Squadron/OSK); Maj Robert Biggers (Detachment 2, 318th Information Operations Group); Maj Jason Keen (US Air Force Judge Advocate General); Maj Joel “Oz” Bieberlie (US Air Force Space Command/A3TW); and Mr. Steven Landes (National Air and Space Intelligence Center).

I would like to give a special thanks to Col John Warden, USAF, retired, for taking time to meet and discuss his air campaign plan. His insight increased my understanding of the enemy as a system concept and directly contributed to this work.

I would like to thank my parents for instilling discipline, initiative, and a persistent drive throughout my early years and for providing constant support to my family during my more than two decades in the USAF. I also

appreciate the many hours they spent reviewing SAASS papers throughout the school year, along with the countless iterations of this work.

To my wife, thank you for your constant support, understanding, patience, and love. When this adventure is done and we are on to the next, it is great to know we have shared every step of the way together.

Finally, I would like to thank my heavenly Father. I rely heavily on His word, specifically Philippians 4:13 (New International Version): “I can do all things through Him who gives me strength.” I will continue to seek His counsel in all I do and pray I use the gifts He has given me according to His will.

Abstract

In this work, I examine historical targeting theories for airpower and their effects on the organizational, training, and equipping functions of the US Air Force. This analysis is intended to develop lessons learned in order to focus on the USAF cyber power organizational, training, and equipping functions. Just as early theorists conceptualized the use of airpower, so must contemporary USAF theorists develop a cyber-power targeting theory to apply in future wars.

Following World War I, airmen at the Air Corps Tactical School (ACTS) developed an “industrial web theory” for targeting to achieve victory through airpower. This theory informed senior-leadership decisions regarding organizational, training, and equipping functions for the USAF throughout its use. The targeting theory was employed with mixed results from World War II through the Vietnam War. In the late twentieth century, Col John Warden conceptualized and validated an airpower targeting theory based upon a concept of the enemy as a system. This model earned its success in Operation Desert Storm and is continually used in doctrine, education and training, and planning today. Although the Air Force went to war with the force it had in the early 1990s, Colonel Warden’s theory informs organizational, training, and equipping decisions for senior leaders today.

A USAF cyber-power targeting theory should consider lessons learned by early airpower theorists and practitioners. Just as Airmen attempted to influence the third war-fighting domain during airpower’s infancy and maturation, Airmen are attempting to influence the fifth war-fighting domain of cyberspace today.

In this work, I evaluate early airpower targeting principles and attempt to draw parallels in order to propose a cyber-power targeting theory. Next, I draw upon limited artifacts inherent to wielding cyber power—attribution, authorities, and centers of gravity—and acknowledge their impacts upon leaders and practitioners of cyber power. Finally, I propose a cyber-power targeting theory based on offense, defense, and exploitation objectives. In addition to focusing on the adversary, the theory is intended to cause introspection in order to identify potential Air Force and national security vulnerabilities in, through, and from cyberspace.

Chapter 1

Introduction

Revolutionary change, fuelled by the information age, is occurring.

—David Lonsdale
The Nature of War in the Information Age

A major battle in a theater of operations is a collision between two centers of gravity; the more forces we can concentrate in our center of gravity, the more certain and massive the effect will be.

—Carl von Clausewitz
On War

On 18 August 2009 the US Air Force (USAF) activated Twenty-Fourth Air Force at Lackland AFB, Texas. The focus of the service's newest numbered air force command was toward emerging requirements of cyberspace operations, retired general C. Robert Kehler expressed.¹ He went on to say that “through the Twenty-fourth Air Force, our service will present a full spectrum of cyberspace capabilities vital to the joint warfighter.”² Thus began the USAF endeavor into what is called the “fifth operational domain” or “new frontier.”³

Since the activation of the Twenty-Fourth Air Force, many questions have arisen regarding USAF cyberspace operations. Is the USAF any further along the path to providing the joint war fighter more operational capabilities within cyberspace than were available in 2009? Is the USAF simply kicking the can down the road regarding operations and capabilities rather than stopping to reflect and evaluate if we structured the force and defined objectives correctly and clearly from the beginning? Has the Department of Defense (DOD) clearly defined objectives for cyber power for the USAF? Has the USAF evaluated ongoing cyberspace operations, and is the Twenty-Fourth Air Force on the path the USAF intended it to travel?

Comments by the Air Force's current chief of staff, Gen Mark A. Welsh III, project a sense of caution as the USAF moves forward in cyberspace. During the September 2012 Air Force Association Air and Space Conference and Technology Exposition, General Welsh said, “I still twitch when I say cyber. I'm a believer. I'm just not sure we know exactly what we're doing in it yet and until we do, I'm concerned it's a black hole.”⁴ His brief comments capture succinctly not only what operators and leadership throughout the USAF are thinking but also potentially what senior leadership throughout DOD and US

INTRODUCTION

civilian corporations ponders as well. These concerns are especially true during a period of fiscally constrained budgets, reduced government and corporate spending, and unknown potential conflicts in the area of cyber—uncertainty regarding the role of cyber in all war-fighting domains.

The good news is that senior military leadership appears to genuinely care where cyberspace operations are going; they are taking proactive measures to enable cyber power efficacy. As recently as December 2012, Lt Gen Michael J. Basla, USAF chief information officer, stated that “the Air Force needs to gain a better understanding of what the military as a whole will require in terms of cyber capabilities.”⁵ He suggested that this understanding would come from the Joint Chiefs of Staff and the secretary of defense, who planned to finalize US Cyber Command’s (USCYBERCOM) requirements.⁶ These comments and actions came within months of USCYBERCOM giving each armed service a list of cyber capabilities it was expected to execute in support of world-wide operations.⁷ Now it appears that decision makers are reviewing these tasks to ensure that known and potential threats within the next decade are being addressed by each service’s required capabilities. The preceding statements signify a general acknowledgment of the extremely dynamic and evolving nature of the cyber domain, far outpacing the rate of change in the other war-fighting domains. This is supported by a constant reminder that cyber is the only man-made domain; the land, sea, air, and space domains are physical and, unlike cyberspace, rather unchangeable.

The questions posed above do not have simple answers, and I do not intend this work to propose their solutions. I do, however, intend to focus on what I call a center of gravity for USAF cyberspace operations—the *theory of Air Force cyber-power targeting*. The intent of this theory is to address the question, *what is the target of USAF cyber power?* More specifically, *does the air-power targeting strategy employed by the USAF apply to the use of cyber power?* The theory proposed could go beyond USAF thinking to the other service components, the DOD, and all national cyberspace functions critical to US national security. It may also aid military leaders in their current thinking about what capabilities military services need to wield cyber power in order to support political objectives of the future. These needs, once determined, should shape the ongoing discussions regarding the organization, training, and equipping of cyber forces.

Cyber targeting and associated doctrine should be the center of USAF cyber strategy and its plans to organize, train, and equip (OT&E) a force for full-spectrum cyberspace operations. Without a clear objective of what the USAF intends to target within cyberspace, whether the focus is defense, offense, or exploitation, it is difficult to understand how an organization can execute op-

erations, how education and training are focused, and how equipment can be procured toward intended objectives. Without a strategic focus regarding what the USAF intends to target with cyber power, one may draw parallels to the famous passage in Lewis Carroll's *Alice in Wonderland*:

Alice came to a fork in the road. "Would you tell me please which way I should walk from here?" she asked.

"That depends a good deal on where you want to get to," responded the Cheshire Cat.

"I don't much care where," said Alice.

"Then it doesn't matter which way you walk," said the Cat.⁸

Understanding what targets cyberspace operations can affect is critical to deliberate planning or crisis planning. Without understanding the target, it is difficult to understand how leaders expect operations to achieve their objective. In order to understand targeting objectives, we must first understand the parameters for conducting cyberspace operations, as currently defined, and then current targeting doctrine regarding DOD operations.

Policy and Doctrine Review

Title 10 is the *US Code (USC)* that governs operations by the armed forces. Military activities in cyberspace are defined within Title 10: "Congress affirms that the Department of Defense has the capability, and upon direction by the President, may conduct offensive operations in cyberspace to defend our Nation, Allies, and interests."⁹ Of course, the above actions are subject to policy and legal constraints that govern the DOD, including the law of armed conflict and Title 50 of the *USC—War and National Defense*.¹⁰ A review of both Title 10 and Title 50 authorities reveals absolutely nothing regarding cyber targeting and what DOD efforts should focus on. In fact, the word "cyber" is mentioned only four times on two pages in Title 50, in which the chief of defense nuclear security is directed to provide for the administration's cybersecurity.¹¹ Given the activation of USCYBERCOM in 2009, one might question whether this Title 50 task still belongs to the chief of defense nuclear security or to the commander, USCYBERCOM. The lesson drawn from this is simply that the political objective for military cyber power endeavors is not clearly found in the *US Code* at this time.

A review of Joint Publication (JP) 3-60, *Joint Targeting*, defines a target as "an entity (person, place, or thing) considered for possible engagement or ac-

INTRODUCTION

tion to alter or neutralize the function it performs for the adversary.”¹² This definition of a target provides focus to a cyberspace operator who is tasked to organize, equip, and train a force required to meet the Title 10 objectives defined above—when focused solely on offensive operations. However, what to target still appears vague. An analysis of Air Force Doctrine Document (AFDD) 3-60, *Targeting*, yields no further explanation. In fact, the last publication of this document from June 2006, which has been updated to incorporate changes as of May 2011, does not contain the word “cyber.”¹³ Somehow the USAF missed including the updated mission of air, space, and cyber when it updated this doctrine.

A continued examination of current doctrine on targeting, and one closer to USAF operations, focuses on Air Force Instruction (AFI) 14-117, *Air Force Targeting*. Although this document was last published in May 2009, three months before the activation of Twenty-Fourth Air Force, the word *cyber* only appears once in the document’s main body. This document delegates responsibility for cyber targeting to Air Force Space Command (AFSPC) when it says, “AFSPC will act as the lead MAJCOM [major command] for space-related and cyber targeting issues.”¹⁴ Given the focus of this AFI on intelligence operations within the USAF, its assignment of responsibility is not faulty. However, it is irrelevant when guiding USAF commanders toward building effective cyber power strategies and capabilities.

Finally, a review of AFDD 3-12, *Cyberspace Operations*, provides the most direct discussion regarding USAF cyberspace operations and targeting with cyber power.¹⁵ Initial document discussions focus on the adversary’s intentions regarding DOD targets, before turning to theater operations. The closest advocacy we find in current USAF doctrine states that during planning, Twenty-Fourth Air Force organizations will use the commander, Air Force Forces (COMAFFOR) or joint force air component commander (JFACC) joint integrated prioritized target list and target nomination list for operations. In other words, USAF cyber targeting objectives are not determined by the unit tasked with conducting USAF cyberspace operations but rather by ongoing theater-level operations. A level of deductive reasoning leads one to conclude that cyber targeting is derived from targeting doctrine for air and space operations that predates the activation of Twenty-Fourth Air Force or USCYBERCOM. Given new warfare capabilities in, through, and from cyberspace operations, it is valid to evaluate a cyber-targeting theory that examines offensive, defensive, and exploitation possibilities beyond existing doctrine.

Literature Review

The academic research I use to support positions within this work focuses primarily on the period from the birth of airpower through today. I review the interwar period, World War II, the Korean War, and Desert Storm to evaluate airpower targeting theories, developing a cyber-power targeting theory for today. Although I utilize many books, periodicals, online articles, interviews, and historical research, the three principal books used for the three time periods discussed are *History of the Air Corps Tactical School, 1920–1940*, *The Air Campaign*, and *Cyberpower and National Security*.¹⁶

Robert Finney's *History of the Air Corps Tactical School, 1920–1940* captures the first efforts by Airmen to think, develop, and document airpower targeting strategies. Beginning with the Air Corps Tactical School (ACTS), senior leaders organized, trained, and equipped the Army Air Corps for airpower operations in World War II and beyond. From the early airpower theorist Billy Mitchell through the men who served at ACTS, the strategic bombing mantra enveloped the service's culture before and after the USAF became a separate service in 1947. This airpower tautology remained throughout the Cold War era until a new airpower strategist emerged.

John Warden, a Vietnam combat veteran, learned early in his career the implications of fighting a war with unclear objectives and without the equipment necessary to achieve them. In *The Air Campaign*, Warden defines a targeting theory that transcends the works of ACTS, while employing early principles of the industrial web theory. Warden developed a five-ring model for an air campaign plan, which served the 1991 Desert Storm Operation. The model receives an update throughout my current work, thanks to a personal interview with Warden. Since Desert Storm, airpower strategists continue to use the works of Mitchell, ACTS, and Warden for all levels of war planning and operations. However, tomorrow's airpower strategists must focus on more than airpower; a focus on cyberspace is required.

Cyberpower and National Security is a compilation of essays regarding cyber power challenges facing the United States. More than 20 authors with varying backgrounds and experience offer relevant cyber power perspectives. From policy recommendations, problem definitions, and preliminary cyber power theories to infrastructure, technology, security, and law enforcement issues, the authors synthesize major challenges facing the United States as the country attempts to wield cyber power in order to influence national security objectives.

Warfare

The character of war will change, but the nature of war does not.¹⁷ Carl von Clausewitz succinctly provides the simplest definition of war: “War is fighting. . . . Fighting, in turn, is a trial of moral and physical forces through the medium of the latter . . . [in which] psychological forces exert a decisive influence on the elements involved in war.”¹⁸ This point is especially relevant today as some theorists, academics, and military and civilian leaders argue cyber war is already under way. This statement is controversial because a declaration of cyber war does not exist, whereas the Hague Convention of 1907 established official protocol for declaring war.¹⁹ This perceived requirement for war has become somewhat convoluted with the rise of nonstate and terrorist actors, in concert with reduced barriers of entry into warlike acts such as flying commercial aircraft into civilian targets. Either way, nations are struggling for dominance in cyberspace—the newest war-fighting domain.

Perhaps the pursuit of cyber dominance today is comparable to the Cold War, in which, after World War II, two superpowers struggled for military dominance. Both the United States and the Soviet Union competed for dominance in the atomic and then thermonuclear power arenas, just as nations such as the United States, China, Russia, France, and others struggle over cyber power today. The difference is that many people today do not believe the struggle for cyber power portrays the same potential for catastrophe as a nuclear holocaust, nor do they perceive an urgency to resolve known cyberspace vulnerabilities. However, a look at history will show that US citizens were not overly concerned about atomic weapons or their threats until the government educated the mass populace, creating an American bunker mentality by raising a public specter of thermonuclear war.²⁰

Arguments can be made that cyberspace vulnerabilities have the potential to cause catastrophic or accidental events if left unprotected or when specifically targeted. For this reason, it is practical to educate society on vulnerabilities created in, through, and from cyberspace, while focusing military operations on specific targets for cyber power use. Until vulnerabilities of targets are exposed, along with their propensity for destruction, the possibility of a “cyber Pearl Harbor” or “cyber 9/11” exists.²¹ This argument does not suggest this level of potential catastrophe will not exist in the future, but at least societies will not be surprised if and when it does occur.

As the United States prepares for cyberspace warfare, whether catastrophic or benign, the public will expect the military to protect citizens from adversaries intent on doing harm—at least from nondomestic threats, given today’s legal constraints. The question for those charged with this protection and who

have the ability to wield cyber power is not simply whether or not the United States can win a war by attacking the national information infrastructure (NII) of an enemy, but rather what is the political objective levied upon the military to achieve?²² Does the military exist simply to protect the sovereignty of the nation and its capabilities? Does cyber power exist for limited war in support of other war-fighting domains? Or should cyber power be a full-spectrum capability for use throughout all phases of military operations and across all warfare domains? Answering these questions will aid in determining what centers of gravity to attack with cyber power in order to meet political objectives.

Foundational Definitions

For the purpose of this study, war is an act of opposing wills pressing upon one another by force or the threat of force, in order to impose one's political objective upon another. This definition is not new but rather derived from varying interpretations of war from well-known theorists such as Carl von Clausewitz, Sun Tzu, and Karl von Moltke.²³ It is critical to start with understanding war before developing a theory for cyber-power targeting if the objectives of targeting are to have a focus. At the same time, a common understanding of war helps readers delineate what is warfare and what is preparation of the battlefield before objectives of war are pursued.

There are as many interpretations of the term "cyber war" as there are observers of the phenomenon. Some of the disparity comes from the fact that cyber war in the new domain is less understood than all of the other warfare domains combined.²⁴ Some of the disparity can be attributed to the various threats within which cyber war exists. Threats vary from the national level (nation-states) to the individual level (hacktivists).²⁵ Dr. John B. Sheldon, professor of space and cyberspace strategic studies at the School of Advanced Air and Space Studies and deputy director of the Air Force Space and Cyber Strategy Center, briefly describes major groups of potential threats.²⁶ Although the threat may vary, the understanding of what constitutes cyber warfare should not. Richard A. Clarke and Robert K. Knake most closely capture the definition of the term *cyber war* as it relates to my work. They state that cyber war is "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."²⁷ While agreeing with this definition, I expand it to include penetration into any portion of the cyberspace domain or other war-fighting domains supported by cyber power with the intent to cause damage or disruption to objects or loss of life.

INTRODUCTION

This association with a loss of life is highlighted in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, in its definition of a cyber attack.²⁸ The *Tallinn Manual* describes a cyber attack as a cyberspace operation, “whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”²⁹

The narrowing of cyber warfare specifically to a nation’s computers or networks is too constrained given the reliance and interconnectedness of DOD operations within cyberspace. Nuclear command and control, military command and control, logistics, transportation, security forces alert and response, federal aviation, financial and medical records, and so on are all interconnected through cyberspace and relied upon by the DOD, commercial industry, and society alike. An attack on the New York Stock Exchange that cripples the nation’s financial network might not be considered an act of war. However, an attack by one nation against another nation’s major oil company that destroys 30,000 computers might be.³⁰ As a nation, the United States should define what constitutes an act of war in, through, or from cyberspace and remove such ambiguity. This point is countered by those who argue that if cyber laws are made unambiguous then nations are required to act against an adversary when a law is violated.³¹

Ultimately, to put cyber war in context, those governing each nation must decide, in concert with their stated policy, while considering international law and precedents at the time, whether a specific cyber attack is defined as warfare. This porous definition is attributed to the newness of the domain and does not account for the concerns today of attribution—being able to identify with certainty who actually conducted the attack.³² The start of cyber war is not as clear-cut as the attack on a row of battleships at Pearl Harbor on 7 December 1941 or the marching of an entire division of troops across the Kuwaiti border, as Iraqi forces did on 2 August 1991.

Although I will expand upon the definition of “center of gravity” in chapter 4, it is important to provide a brief introduction to the concept up front. According to Clausewitz, identifying the centers of gravity is the first task in planning for war.³³ Applicable both to war and targeting, identifying centers of gravity enables efficacy in operations. This is true in cyberspace operations just as in land, sea, air, and space operations. If organizations pursue capabilities (i.e., weapons or weapon systems in the case of a military) or conduct education, training, or exercises without identifying objectives, why should they expect to achieve desired results?

Since the focus is on military objectives—and in a democratic nation like the United States, military objectives are always politically oriented—the targets of any military objective should be focused on centers of gravity, the sources

of power that provide moral or physical strength, freedom of action, or will to act.³⁴ As JP 5-0 suggests, the priority of effort should be directed at the enemy's center of gravity for a decisive response.³⁵ Clausewitz would say that "it is against these [objectives] that our energies should be directed . . . [as the] center of gravity is always found where the mass is concentrated most densely."³⁶

As theories of warfare mature and interpretations vary, my definition of *center of gravity* takes into account the works of Dr. Joe Strange, professor of strategic studies at the US Marine Corps War College, as well as the references provided above. Strange's work toward bridging the gap between analyzing centers of gravity and their associated critical vulnerabilities by introducing critical capabilities and critical requirements is instrumental.³⁷ This is especially evident in the age of cyber warfare, where centers of gravity are not necessarily determined by concentrated mass as suggested by Clausewitz but rather by the interdependence of mass and operations supported in, through, or from cyberspace operations. Therefore, the working definition of *center of gravity* for this work is the source of power that interconnects and enables psychological, moral, or capabilities/physical strength, freedom of action, or an adversary's will to act. Although this definition is only a minor change from the joint definition cited above, it recognizes that there is potentially more than one center of gravity; the connectedness of mass and operations may be a center of gravity. It therefore opens the door for potentially greater psychological impact on the will of an adversary and possible exploitation to potentially prevent or rapidly conclude an ongoing war. This will become more apparent throughout this work, as I believe cyber power is an effective psychological warfare tool—in addition to being a supported, supporting, and decisive capability provider relative to the other war-fighting domains, depending on the desired objective.

Research Intent

With the nature of war, cyber warfare, and center of gravity defined, this paper develops a cyber-power targeting theory that helps shape USAF objectives to organize, train, and equip its cyber forces. A historical review will determine lessons learned from the latest domain used for warfare. Note that space is often referred to as the most recent domain for use by the military; however, space is acknowledged as not being weaponized for warfare. Thus, comparisons to the air domain are appropriate here.³⁸

INTRODUCTION

In chapter 2, I evaluate the ACTS studies on the industrial web theory to gain an understanding of airpower and its intended targeting effects during war. There are well-documented studies on how early airpower strategists and senior military leadership around the world focused solely on strategic bombing as the dominant use for airpower. After World War II, it became apparent to some that changes were needed in aircraft, technology, training, and bombing tactics, techniques, and procedures if airpower was going to be the dominant form of warfare. When we review the early history of airpower, questions surrounding cyber power arise. Are cyber strategists faced with constrained advocacy for cyber power capabilities? Or is the aperture opened fully to exploit all possibilities within cyberspace?

In chapter 3, I continue a historical examination of airpower through a modern lens. An analysis of Col John Warden's look at airpower in the twenty-first century provides an understanding of his five rings, particularly the rings' use in the theory of military strategic attack. As cyber strategists apply Warden's theories to the cyberspace domain, commonalities will likely be found in some areas but not in all. By understanding those commonalities, military strategists can perhaps avoid repeating mistakes and apply lessons learned through trial and error, while avoiding the cookie-cutter approach of collectively applying theories from other domains to the military's newest war-fighting domain. As with any new warfare capability, ongoing challenges in organization structure, manning, technology, domestic and international legal realms, education and training, and interservice collaboration will persist for some time.

In chapter 4, I highlight artifacts relevant to cyberspace operations. Specifically, I discuss the challenges of attribution and authorities, while acknowledging the required understanding of centers of gravity in cyberspace operations. Just as challenges existed when the effects of airpower were unknown, constraints exert themselves on the potential impacts of operations within cyberspace. Understanding these challenges may help answer similar questions developed in the early days of airpower, while pressing cyberspace warriors to consider new ones not yet discussed. If efforts to continually enhance cyber domain capabilities address questions that inhibit operations today or potentially constrain future operations from achieving desired effects, those efforts will be successful. If cyberspace operators and strategists can discuss and debate serious questions such as "what will cyber domain operations look like when the challenge of attribution is resolved?" or "can the barriers to entry into cyberspace operations be elevated to reduce potential threats?," defenders of this nation's freedoms will be doing their job.

In chapter 5, I propose a cyber-power targeting theory that incorporates applicable lessons learned from other warfare domains while adding thoughts specific to cyberspace operations. Unlike some early airpower advocates, my position is not that cyber power is the dominant form of warfare. Nor do I ascribe to an extreme advocacy or debate over which form of cyber warfare—offensive or defensive—is the more capable position in cyberspace operations. However, I do suggest more focus be placed on attributed offensive operations. This acknowledges that cyberspace operations require more flexibility between offense and defense than any other form of warfare and that cyberspace operations are as capable of executing a supporting role, a supported role, or an independently decisive role in war. For these reasons, cyberspace operations require resources equal to those of the air, land, sea, and space domains if cyberspace operations are truly going to be a capable military means to achieve political objectives.

In chapter 5, I further develop the proposed cyber-power targeting theory, applying it to potential US homeland threats with the intent to highlight national security concerns. The potential threats drive a discussion about organization structures, education and training, and policies that leads to the following questions: Is the United States organized to fight cyber warfare? Are taxpayer dollars being wasted by multiple agencies within the United States conducting similar functions? Who is the driving authority for cyber policy within the United States, and under what authority is retribution for noncompliance achieved? Because this paper's scope is developing a cyber-power targeting theory, these questions are cursory in nature. Their intent is to stimulate thinking regarding potential changes in how US organizations manage critical national security infrastructure that can be manipulated by an adversary's cyberspace operations.

Beyond the Scope

It is important to address up front a few areas that I do not spend time discussing in this paper. The intent to develop a cyber-power targeting theory should be clear by now. However, the development of the tools to affect the targeting objectives is not my focus. In other words, for airpower, it is important to discuss whether laser-guided munitions or a nuclear bomb is applicable to destroy a specified target. It is also important for the planners of an air tasking order to determine what aircraft is best suited to conduct a mission. Other requirements must be determined as well: the kind of support needed from intelligence planners for intelligence preparation of the battlefield, the logistical

INTRODUCTION

support for ensuring munitions are on hand, and the right maintenance personnel for mission aircraft. Although these are vital and needed for effective and efficient air operations, their focus is on the weaponry needed to support airpower in meeting its targeted objective. All of these same concerns exist for cyber power and must be addressed by strategists planning cyberspace operations. However, I advocate that all of those considerations follow the determination of a cyber-power targeting doctrine. Once the USAF determines what it wants to target—whether for offense, defense, or exploitation—then it can perform all other support functions necessary to enable defined objectives, including building the weaponry required.

Debates over whether electronic warfare or the use of the electromagnetic spectrum is vital to cyberspace operations are beyond my scope as well. I agree with Daniel Kuehl's definition in that cyberspace includes the electromagnetic spectrum, with the caveats that the true domain is the electromagnetic spectrum and that cyber power is wielded through the man-made infrastructure that enables effects in that domain.³⁹ This is also why I believe the USAF should consider combining inherent electronic warfare capabilities with the Twenty-Fourth Air Force to harmonize cyberspace energies. However, that too is beyond the scope of this paper.

I suggest there should be serious consideration and evaluation of cyberspace operations. If the consolidation of money, manpower, and operations is limited by antiquated paradigms or stovepipe thinking based on saving the military our fathers grew up in, then USAF leaders are failing in their primary objective, which is the defense of our great nation and not the preservation of the military service in which we serve. This does not mean we can reduce or eliminate all duplication, and sometimes it will make sense to keep operations separate between different military services. However, where it makes sense, consideration should be given to consolidating operations where excessive collaboration drives inefficiencies. Can we truly recognize today's inefficiencies without defining the cyber target of each service, DOD, and national cyberspace operations and the intended projection of cyber power? We do not build a ship, a tank, an aircraft, or a satellite without a strategic objective in mind. Should we manage military cyberspace through a similar lens?

Summary

In this chapter, I suggest questions for cyber strategists in today's USAF to consider. I also recommend that the focus for such strategic thinking revolve around targeting an adversary's will and capabilities to fight. Cyber power is

not limited only to activities within the realm of cyberspace itself, but rather any diplomatic, informational, military, or economic instrument of power as well as any commercial, industrial, or other societal capability supported in, through, or from cyberspace. Simply put, from a military perspective any land, sea, air, space, or cyber capability that employs cyberspace in any way has the potential for disruption by an adversary's cyber power if left vulnerable.

By defining possible targets of potential foreign and domestic adversaries, the USAF can establish a trajectory to OT&E forces for offensive, defensive, and exploitation operations. Today's USAF cyber power traditions are similar to the motto of the men of the Army Air Corps in the 1920s: *Proficimus More Irretenti*.⁴⁰ The possibilities are boundless, but with constrained budgets and rapidly changing technology, the USAF must pursue specific objectives and not leave the first war initiated and/or dominated by cyberspace operations to chance. Looking back at how early airpower advocates shaped the future of airpower might offer valuable lessons for cyber power strategists of today.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. General Kehler was the Air Force Space Command commander at the time Twenty-Fourth Air Force was activated.
2. Carla Pampe, "Air Force Activates Cyber Numbered Air Force," Air Force Space Command, 18 August 2009, <http://www.afspc.af.mil/news/story.asp?id=123163863>.
3. Welch, "Cyberspace—The Fifth Operational Domain," 2–7. Also see former secretary of defense Leon Panetta's 2012 speech to veterans and business executives at the Intrepid Sea, Air and Space Museum in New York, quoted in Zachary Fryer-Biggs, "Panetta Lays Out New Cyber Policy," *Defense News*, 12 October 2012, <http://www.defensenews.com/article/20121012/DFREG02/310120002/>.
4. Welsh, "Speech to the Air Force Association."
5. Jared Serbu, "Air Force Role Just 1 Piece of DOD's Cyber Puzzle," *Federal News Radio*, 3 December 2012, <http://www.federalnewsradio.com/398/3140801/Air-Force-gels-around-its-cyber-future>.
6. Ibid.
7. Reed, "Pentagon Is Tweaking the Cyber Capabilities."
8. Carroll, *Alice's Adventures in Wonderland*, 89.
9. Conference Report on H. R. 1540, *National Defense Authorization Act*.
10. Ibid.
11. Title 50, War and National Defense.
12. JP 3-60, *Joint Targeting*.
13. AFDD 3-60, *Targeting*.
14. AFI 14-117, *Intelligence*.
15. AFDD 3-12, *Cyberspace Operations*. This publication was rescinded 31 October 2013.

INTRODUCTION

16. Finney, *History of the Air Corps Tactical School*; Warden, *Air Campaign*; and Kramer, Starr, and Wentz, *Cyberpower and National Security*.

17. Clausewitz said that “the art of war is the art of using the given means in combat; there is no better term for it than the conduct of war. The art of war includes all activities such as the creation of the fighting forces, their raising, armament, equipment, and training.” Clausewitz, *On War*, 127. A more contemporary summation of war is offered by Lonsdale in *Nature of War*, 2. Therein he states that “war is a purposeful act of actual or threatened physical violence which takes place within a dialectic relationship.”

18. Clausewitz, *On War*, 127.

19. See “Opening of Hostilities” in the *Hague Convention*.

20. Craig, *Destroying the Village*, 41 and 148.

21. Fryer-Biggs, “Panetta Lays Out New Cyber Policy”; and Brig Gen Bradford Shwedo, director of intelligence, Air Combat Command, interview by author, Maxwell AFB, AL, 2 November 2012.

22. David Lonsdale’s reference to NII focuses on warfare that is kinetic destruction, compared to disruption of capabilities, which leads to a desired strategic effect. Both are capable products of cyber warfare given the authorities, intelligence, and tools. Lonsdale, *Nature of War*, 135–36.

23. Clausewitz defines war as a trinity (primordial violence [people, chance, and probability]; commander; and element of subordination—instrument of policy). Clausewitz, *On War*, 89. Sun Tzu states that “war is a matter of vital importance to the state” and must be appraised in terms of five factors: moral influence, weather, terrain, command, and doctrine. Sun Tzu, *Illustrated Art of War*, 91. Karl von Moltke defines war as rough and violent but goes on to say that a rapid conclusion of war undoubtedly constitutes the greatest kindness. Moltke, *Moltke on the Art of War*, 22–24.

24. To read a paper on understanding key features and types of cyberspace operations and conflicts, see Office of the Director of National Intelligence, *The IC and Cyberspace*, 193.

25. Hacktivists are tech-savvy activists who utilize computer networks to promote political agendas, often leaking sensitive government intelligence after illegally accessing stored data.

26. Sheldon, “State of the Art,” 6–11.

27. Clarke and Knake, *Cyber War*, 6.

28. The *Tallinn Manual*, written by an international group of experts including well-respected legal scholars and practitioners with expertise in cyber issues, is a scholarly nonbinding study examining the application of international law to cyber conflicts and cyber warfare. Schmitt, *Tallinn Manual*, 106.

29. Ibid.

30. “Israel Builds Up Its Cyberwar Corps,” *UPI*, 2 November 2012, <http://www.upi.com/BusinessNews/Security-Industry/2012/11/02/Israel-builds-up-itscyberwar-corps/UPI-52421351881449/>.

31. Maj Gen Charles Dunlap, USAF, retired, argues cyber laws should be left somewhat ambiguous so that it is a political decision to react or not, rather than a forced situation in which leaders must respond. I argue that whether laws are ambiguous or unambiguous, war remains a political decision. In the Western way of thinking, militaries do not react when a law is violated without approval from civilian leadership. The reality is, unambiguous laws afford adversaries room to maneuver that they might not otherwise have with defined laws. Dunlap, “Perspectives for Cyber Strategists,” 81.

32. For concerns about attribution and recommendations for addressing these ongoing concerns, see Lin, Allhoff, and Rowe, “Is It Possible to Wage a Just Cyberwar?” Some pundits suggest mandating that all cyber attacks should carry a digital signature of the attacking orga-

nizations. This is a utopic idea, and the ability to enforce it borders on the impossible without international standards and a policing force to ensure compliance.

33. Clausewitz, *On War*, 619.

34. JP 5-0, *Joint Operation Planning*, 250.

35. *Ibid.*, 222.

36. Clausewitz, *On War*, 485 and 596.

37. Rueschhoff and Dunne, "Centers of Gravity," 120.

38. For details regarding the establishment of an international agreement for banning the placement of all weapons of mass destruction in orbit around the earth, see information on the 1963 United Nations General Assembly Resolution 1884 in Morgan, *Deterrence and First-Strike Stability in Space*, 9.

39. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Kramer, Starr, and Wentz, *Cyberpower and National Security*, 28–31. The author states that cyberspace is the "operational use of electronic technologies and the electromagnetic spectrum to create, store, modify, exchange, and exploit information and [systems] through networked technologies." I believe cyberspace will be used to prevent the use of, and potentially destroy, information and systems supported or controlled through cyberspace in the future as well.

40. The Latin is translated as "we make progress unhindered by custom."

Chapter 2

From Airpower Development to Targeting the Industrial Web

The Goddess of Change was turning her disturbing attention to the sky. The first great boom in aeronautics was beginning.

—H. G. Wells
The War in the Air

From the time when fictional writers spurred thoughts in children and adults alike until bombs reigned down from the sky in actual warfare, a plethora of possibilities existed as to what the invention of aerial flight would bring to warfare. Despite claims that the first military use of aerial devices came from the Chinese invention of the kite in approximately 200 BCE, and excluding balloon use in warfare, it is safe to proclaim effective military use of aviation did not occur until after the first manned aircraft flight of 1903.¹

This chapter describes US aircraft development from infancy to its use in warfare. The focus is not on the wars themselves but rather the intended use of military airpower compared to doctrine of the time. Questioning whether technology of the time enabled objectives is relevant—as is gaining an understanding of leadership agendas and expectations for the role of airpower compared to conventional thinking. What shaped these thoughts and actions? What drove changes in thinking? How was airpower enabled to achieve a dominant role in warfare as theorists such as Giulio Douhet, Hugh Trenchard, and Billy Mitchell claimed was possible?² These theorists and the practical application of airpower in World War I shaped doctrine and the use of airpower in subsequent wars.

Following a brief history on early rules of airpower and airpower development, I delve into the chapter's primary focus of understanding the industrial web theory as it relates to targeting objectives by aircraft during war and peace. How and why was this theory developed? What was its focus? How did it affect US airpower doctrine, strategic thinking, and operations within the Army Air Corps of the day? Did the focus on strategic bombing of vital centers aid technology development while blinding senior leaders to airpower limitations? A case study of World War II rounds out the chapter by highlighting relevant aspects of airpower abilities and limitations during these early years and how airpower established the framework for strategic targeting in the future.

International Rules: Fear of Airpower

By 1899 a pervasive attitude that balloons would “be used to drop explosive substances” led to an international agreement and “five-year ban inhibiting a projectile or explosion from a balloon.”³ However, this prohibition did not prevent military tacticians from considering the possibilities of aerial warfare during the time of the ban. However, it possibly slowed the technological development of weapon systems and potentially limited the thinking about roles and missions for airpower in the next major war: World War I.

The 1899 ban expired, and the rules were not updated until three years after World War I. However, the Hague Draft Rules of 1923 provided no absolute regulation or binding international law regarding targets for bombing by airpower.⁴ Although not adopted, the draft rules did serve as an example of customary international law, whereby nations observe the rules of custom rather than a formal convention. As international law evolved, so too did airpower strategy. Early twentieth century theorists, fictional writers focused on heightening awareness, and those with limited experiences of airpower in warfare each had their role in shaping airpower thinking toward future conflict. For the United States, a group of men at the Army Air Force ACTS shaped early US airpower strategy. Theorists such as Douhet, Trenchard, and Mitchell, who—as demonstrated by their writings—were deeply affected by their experiences from World War I, shaped the thinking about airpower at ACTS. The result of such thinking was a daylight bombing strategy that guided the application of US airpower in subsequent wars.

Shaping Strategic Bombing Doctrine

The perceived psychological impact upon residents of aerially bombed cities was at the foundation of the formulation of strategic bombing doctrine. Although such perceptions were mostly exaggerated rhetoric, given the primitive bombing technology of the day, the ambition was not unfounded. In 1849, during an Italian revolt against the Austrian Hapsburgs, Austrian imperial forces bombed Venice from the air with projectiles carried by small linen and paper balloons.⁵ These attacks were rudimentary in nature but effective as propaganda extolling the “frightful effects” of such new weaponry. After the advent of manned aerial flight in 1903, exaggerations regarding the potential of airpower proliferated due to the works of fiction writers like H. G. Wells. Additionally, French newspapers published articles focused on how French bombing would obliterate Berlin, heightening airpower awareness. Furthermore,

airpower advocacy gained importance after the small wars in Libya during 1911–12 and when the French quelled an uprising of Morocco in 1912.⁶ It would not be long before political representatives raised national concerns regarding airpower devastation through publications of their own.

Years before World War I, a British parliamentarian, William Joynson-Hicks, published an article in the *National Review* titled “Command of the Air.” Aside from confirming for British citizens that bombs and bullets could be delivered from airplanes, Joynson-Hicks outlined a strategic role for the bomber.⁷ He stated that bombers would target material resources to deprive their use, strike at “nerve centers,” government buildings, railways, and stock exchanges and attack the population to affect the morale of the people.⁸ Thus began foundations of a strategic bomber doctrine that the Royal Air Force (RAF) would employ in various forms in subsequent wars. In reality, the strategic bombing strategy Joynson-Hicks advocated was not limited to the RAF.

In early 1915, during World War I, the French military had more than 120 aircraft prosecuting long-distance attacks on German industrial sites determined as vital to German war efforts. The intent was similar to what Joynson-Hicks advocated: reducing the adversary’s material resources for war. Although French bombers executed attacks on vital German centers, the French bombing theory stated that air forces were to cooperate with ground forces, eroding the enemy’s will and capabilities.⁹ This relegated the potential capabilities of airpower throughout the war and limited airpower’s potential. The US Army Air Corps would experience the same challenge.

In executing air warfare in World War I, the Royal Flying Corps (RFC) of Britain helped the French in 1914 and beyond. Whether following the recommendations of Joynson-Hicks or of his own accord, Hugh Trenchard of the RFC employed airpower to meet objectives he determined would have an effect on the adversary’s abilities to wage war. Notice the subtle change between Joynson-Hicks’s focus on morale and will and Trenchard’s focus on the capabilities to wage war. Trenchard’s actions had great influence on British airpower and its history after World War I.¹⁰

During the Somme campaign, Trenchard directed RFC pilots to fight offensive air battles in order to win maneuverability for British reconnaissance, artillery, and other ground support aircraft—while denying the enemy the freedom to do the same. Reflecting on his experiences from World War I, Trenchard opined that the airplane ought to be used as an offensive and not a defensive weapon. Thus airpower became what Joynson-Hicks advocated, and a new foundational body of British air theory existed for use during and after the war.¹¹ These theories extended to US airpower thinking as well.

American airpower prior to entry into World War I in 1917 did not have firsthand experience of long-range bombing.¹² Although the Wright brothers piloted the first documented powered, heavier-than-air manned flight, the United States took a leisurely approach to developing and exploiting military applications of aircraft. By 1907 the US Army established the Aeronautical Division within the Signal Corps, but by 1911 this corps only had one aircraft and one pilot.¹³ Besides the minimal force structure, the doctrine for aircraft employment was minimal in defining expected roles of aircraft in military operations. The US War Department's *Field Service Regulations of 1914* stated aviation was for reconnaissance and observation of artillery fire, and by 1916 aviation was still bound to ground troops.¹⁴

In April 1917 Col William "Billy" Mitchell arrived in Europe, where he would begin his advocacy for airpower and go on to become the most influential American aviator of the war.¹⁵ After being promoted to brigadier general and appointed chief of Air Service, Army Group, Mitchell advocated for aviation to become a separate branch like infantry and artillery, arguing aviation would have a greater influence on the ultimate decision of war than any other military arm.¹⁶

Collectively the major allies of World War I—Britain, France, and the United States—established and attempted to exercise certain principles for the employment of airpower. The allies recognized that aerial superiority was a prerequisite to successful air operations, that a determined offensive against hostile forces to gain and maintain control of the air was essential, and that focused air attacks on enemy rear positions would reduce enemy air attacks on frontline friendly forces. Additionally, the allies understood that limiting air services to reconnaissance and observation failed to utilize aircraft fully and that the air arm was more effective under a single commander.¹⁷

Analysis of Airpower in World War I

According to RAF history, the airplane's role in World War I was reconnaissance; later uses were consequences of purposes and logic of events.¹⁸ In other words, aviators found useful war applications for airpower when situations arose. Maj Gen Benjamin Foulois told interviewers that "we always had ideas about using the airplanes as offensive weapons, which was contrary, of course, to military policy at the time."¹⁹ This highlights ongoing attempts by operators at the tactical level to apply innovative solutions to operational challenges. Once operators find tactics, techniques, and procedures that

work—especially in warfare—airmen will institute new actions as standard procedure even though current doctrine or policy may not reflect the action.

Following the war, despite airplanes being employed as “little more than [an] extension of existing weapons,” it was evident to war fighters that the character of war had changed.²⁰ Maj Gen Haywood S. Hansell, Jr., later stated that “the potential application of military force through mass employment of aircraft was recognized in World War I.”²¹ Acknowledging this change, Congress enacted the *Army Reorganization Act of 1920*, creating the Air Service as a combat arm within the Army.²²

The need to train officers in military aircraft employment was among the first objectives sought by leaders of the new Air Service; thus, the Air Service Field Officers’ School was activated at Langley Field, Virginia, in 1920. The school changed names to become the Air Service Tactical School in 1922 and then the Air Corps Tactical School in 1926 when it moved from Langley Field to Maxwell Field, Alabama. Despite the name changes, the goals of the school were the same following World War I—train air officers in the strategy, tactics, and techniques of airpower.²³

ACTS and the Industrial Web Theory

The Air Service was not only the newest combat arm of the Army—responsible for developing training and educating officers in the newest warfare domain—it also had no airpower doctrinal history to use as a foundation for the ACTS course. Therefore the school focused on educating and training air officers and developing air doctrine.²⁴

Prior to 1926 military doctrine focused on surface engagements. The Air Corps issued its first doctrine, which appeared as training regulation (TR) 440-15, *Fundamental Principles for the Employment of the Air Service*, on 26 January 1926.²⁵ The gist of this doctrine, which acknowledged that there may be special needs that take air forces away from ground forces, was that airmen aided ground forces to gain success.²⁶ Despite revisions, the doctrine largely remained the same until 1940. However, this did not deter airpower activists from exploring the boundaries of airpower’s use.

Between 1926 and 1933, practitioners of airpower realized an air force enabled commanders to strike more quickly and decisively at an enemy’s bases and centers of concentration.²⁷ This line of thinking prevailed, and instruction at ACTS stated that air force objectives should be focused on destroying the enemy’s military strength in the areas of a hostile air force, troops, supplies, and lines of communications (LOC) in the combat zone; concentration

centers and LOCs in the communication zone; and industrial and transportation centers in the zone of interior.²⁸

As training and doctrine advanced through ACTS courses of instruction, the air officers' thinking continued to expand. In 1933 a movement surfaced that moved beyond thinking about pursuit aircraft—fighter aircraft in today's lexicon—and more toward bomber aircraft surfaced. Maj Donald Wilson, ACTS course instructor, was one of the first instructors credited with preparing a course focused on attacking grounded hostile aircraft.²⁹ This line of thinking defined targets within the interior of an enemy's country as bomber objectives; the target's destruction would disrupt the entire fabric of an enemy's economy and thereby disrupt the normal day-to-day function of society.³⁰

From 1935 to 1940, ACTS continued to refine targeting focus, studying the American industrial structure to determine geographic centralization of industry, the component parts of industry, the importance of various parts, and the vulnerability of industry to air attacks. The result of this research came to be known as the industrial web theory or the targeting objectives of strategic bombing as determined by ACTS.

Up to this point in history, US military doctrine was "set forth in the Field Service Regulations of 1923" and focused on destruction of the enemy's armed forces.³¹ ACTS recognized that in the past, "except in unusual circumstances, an enemy's capital, commerce, industrial centers, or resources had not been considered proper military objectives."³² ACTS determined that the limited military objectives were due to limited military power of the day. However, with the advent of airpower and the ability to operate in the third dimension, a belligerent country's entire population could be targeted. "In short, using airpower to strike vital points of a nation's structure . . . [was] a means of achieving the military objective with the least possible cost."³³ Moving away from targets that hinged on ground strategy warfare, Major Wilson focused airpower on targets in the interior of an enemy's country. His intent was to identify targets that "would disrupt the entire fabric of an enemy's economy and thereby to discommode the civilian population in its normal day-to-day existence and to break its faith in the military establishment to such an extent that public clamor would force the government to sue for peace."³⁴ Therefore, ACTS viewed transportation, steel, iron ore, and electric power complexes as air force objectives. By attacking these targets, the industrial fabric of a nation would collapse; thus, the industrial web theory was born.

From a contemporary perspective, Robert Pape, in *Bombing to Win*, captures the intent of the industrial web theory. The industrial web tied in several key producers, including basic industry and its sources of raw materials, plant machinery, power supplies, and the workforce. The thread that tied workers

to the web was called the industrial fabric: sources of food, clothing, and utilities. Since industrial economies were thought to be fragile, it was believed that a small number of bombers could destroy the entire economic base of an enemy, wreaking havoc on both civilian welfare and an opponent's military power.³⁵

With a US airpower targeting theory, created by airpower advocates and being taught in the premier airpower school, the only thing left was to put the theory to the test. However, before evaluating history to determine if the theory met its intended objectives, it is valid to ask what impacts the theory under development had on the organization, education, training, and equipping of the US armed forces? Did the hypothesized theory shape the Army Air Corps between the two world wars and, if so, how?

Organizing, Training, and Equipping: Supporting Targeting Theory

Unlike other air forces around the world such as the Luftwaffe, which was created during the interwar years, and the RAF, which was created during World War I, the US Air Force did not become an independent service until after World War II.³⁶ Limited military resources during the lean interwar periods were a major factor contributing to the delayed US response in creating an independent Air Force. The Navy and Army were the traditional US military force providers, and neither service sought to create a separate Air Force. Combined with US policy makers' stated "isolation policy" of the day, there was no real civilian push for the independent force either.³⁷ Ultimately, early airpower advocates received limited organizational change to support the newest warfare domain. Despite this organizational arrangement, new warfare theories developed into doctrine during the interwar years and guided the use of airpower at the onset of World War II.

The term "aspirations" succinctly summarizes the training to test the targeting theories espoused by ACTS. Competing interests among the services, limited aircraft assets in the Army Air Force inventory, skepticism of airpower capabilities, and contemporary Army doctrine of the day that stated air forces support ground forces resulted in limited training opportunities with combat aircraft. For this reason, the application of airpower during World War II, rather than US military training, would initially validate tactics, techniques, and procedures. The belief was that, in the absence of effective tactics, techniques, and procedures, airmen would develop new ones to meet real-world challenges.

At the "onset of the Great Depression" and with diminishing thoughts during the interwar period that the United States might go to war "with the

bomber as its foremost weapon,” military aviation did not drive much technological change or innovation—at least not independently within the military.³⁸ “On the contrary, economic disaster encouraged Americans to see in the rapid growth of commercial aviation a rare glimmer of vitality,” historian Michael S. Sherry stated.³⁹ Airlines in the United States began to expand rapidly and innovatively, including commercial passenger carrier, agricultural, and postal services. Together Army and Navy aviation, alongside commercial industry subsidized by the government, grew the range and power of military aviation. Technological advances led to new bombsights, the first bomber (the Martin B-10), and the four-engine Boeing B-17 Flying Fortress bomber. The latter boasted a 2,400-mile range.⁴⁰ Commercial innovations such as these made the ACTS doctrine of precision bombing possible. Without these innovations, doctrine to guide organize, train, and equip objectives would not have become a reality.

The doctrine, ideas, and initiatives formulated by ACTS were at the forefront of organizing, training, and equipping the US Army Air Corps in the interwar years. It is this point that highlights the anticipated conclusion of this paper. When targets are identified and objectives are clearly defined, then organizing, training, and equipping can follow within a descriptive model. This does not suggest that strategists and war-fighting capabilities get stuck on a model but rather that they meet political objectives by defining strategic targets of an adversary as a logical starting point for developing war-fighting capabilities. Even when US air forces were not independent of other military forces, the potential of airpower was discussed, evaluated, taught, and built. Airmen tested airpower’s capabilities, and those theories and applications that withstood the testing emerged refined and pertinent. Those that did not were relegated to irrelevance and discarded. Incidentally, for the United States and airpower advocates, the opportunity for validation was just around the corner, as the United States and its allies rose to confront Adolf Hitler’s desire for *Lebensraum* and his challenge to the perceived threats of liberalism, capitalism, and democracy represented by American hegemony.⁴¹

Case Study: Employing the Industrial Web Targeting Theory

As airpower evolved after World War I, new airpower theorists abounded. Before reviewing the air war planning documents for World War II and evaluating the effectiveness of the ACTS industrial web theory, it is relevant to highlight an additional airpower theory whose prevalence increased at the start of World War II.

At the onset of American engagement in World War II, Alexander de Seversky, a veteran who served as a naval aviator during World War I, highlighted 11 airpower principles. Although his book *Victory through Airpower* was not published until 1942, de Seversky's principles undoubtedly shaped the thinking of airpower advocates of the day. My intent in highlighting his principles is not to suggest that they shaped warfare planning directly but rather to illustrate that these principles did capture the contemporary airpower advocates' intentions, which overly displayed airpower's role. This zealotry potentially led to divisiveness among military forces rather than creating harmony. Regardless of perception, de Seversky provided a consolidated list of principles that captured what airpower theorists of the day claimed as the most significant lessons of modern airpower.

1. No land or sea operations are possible without first assuming control of the air above.
2. Navies have lost their function of strategic offensive.
3. The blockade of an enemy nation has become a function of airpower.
4. Only airpower can defeat airpower.
5. Land-based aviation is always superior to ship-borne aviation.
6. The striking radius of airpower must be equal to the maximum dimensions of the theater of operations.
7. In aerial warfare the factor of quality is relatively more decisive than the factor of quantity.
8. Aircraft types must be specialized to fit not only the general strategy but the tactical problems of a specific campaign.
9. Destruction of enemy morale from the air can be accomplished only by precision bombing.
10. The principle of unity of command, long recognized on land and on sea, applies with no less force to the air.
11. Airpower must have its own transport.⁴²

De Seversky's principles, combined with those of early airpower theorists, undoubtedly shaped the use of airpower in World War II and beyond.

The United States entered the combat operations of World War II on 7 December 1941, after Japan bombed Pearl Harbor. Up to this point, the United States had maintained its isolation or neutrality policy and, while not at war, achieved

economic benefit through the *Lend-Lease Act* of 1941. This act enabled the United Kingdom to sustain its war efforts against Germany after France fell and the British were financially exhausted. Although the United States offered this program to the global market, it was the Allied forces that reaped the benefits of America's industrial might. During this same period, after observing Hitler's expansionist endeavors through military force, Pres. Franklin D. Roosevelt and his administration took steps to transform the United States into a pre-eminent military superpower, while moving toward a strategy of future air war to defeat Germany—with mass production of aircraft and aero engines.⁴³

Upon entering the war, the United States maintained the attitude the United Kingdom had at the beginning of the war: the bomber would always get through, and high-altitude daylight bombing would be effective in targeting the industrial fabric of Axis powers.⁴⁴ Although the United States changed its operations, adding fighter escorts to bombers and transitioning to night bombing raids to increase the survivability of long-range bombers, the focus was on the efficiency of airpower targeting and its effectiveness at ending war. Authored with input from instructors at ACTS, the United States created plans, known as air war planning documents, to meet these objectives before the country entered the war.

Air War Planning Document (AWPD) 1 was the first US strategic campaign planning document for air war against Germany and Japan written before the attack on Pearl Harbor. It was written by a task force comprised primarily of four officers working in Gen Henry “Hap” Arnold's Air War Planning Division, which had stood up less than a month earlier. Col Harold L. George, chief of Air War Plans Division, along with Lt Col Kenneth Walker, Maj Laurence Kuter, and Maj Haywood Hansell, Jr., rounded out the planning team. All previously served as directors or instructors at ACTS.⁴⁵ The prevailing attitude that pervaded AWPD 1 was that the proper application of strategic bombing would destroy the enemy's will to resist, while its planners strove to address the following air tasks:

- To conduct a sustained and unremitting air offensive against Germany and Italy to destroy their will and capability to continue the war and to make an invasion either unnecessary or feasible without excessive cost.
- To provide air operations in defense of the Western Hemisphere.
- To provide air operations in Pacific defense; to determine the nature of our operations and size of our forces needed, in conjunction with the Army and Navy, for defense of US territories.

- To provide for the close and direct air support of the surface forces in the invasion of the Continent and for major land campaigns thereafter. Large tactical air forces would be required for this task, when the Army was ready for invasion.
- To calculate total air requirements for accomplishment of all these tasks.⁴⁶

These air tasks focused on five objectives determined by the Air War Plans Division:

1. To conduct air operations in defense of the Western Hemisphere
2. To prosecute as soon as possible, after the commencement of war, an “unremitting and sustained air offensive against Germany”
3. To support a strategic defense in the Pacific Theater
4. To provide air support for the invasion of the European Continent if that should be necessary, and to continue to conduct strategic air operations thereafter against the foundations of German military power and the German state until its collapse
5. After victory over Germany, to concentrate maximum airpower for a strategic air offensive against the home islands of Japan.⁴⁷

Following the United States’ entry into World War II, AWPDP 42 was created, drawing from AWPDP 1 and other planning documents. AWPDP 42 called for the US Army Air Force to concentrate on the systematic destruction of the German military and industrial machine through daylight precision bombing while the RAF attacked industrial areas at night to break down morale.⁴⁸ AWPDP 42 was written as a wartime production document and as a counter to the Luftwaffe successes, after President Roosevelt requested aircraft superiority over the enemy.⁴⁹ The plan was General Arnold’s response to the president’s request calling for an air offensive against Europe to deplete the German air force, destroy the sources of German submarine construction, and undermine the German war-making capacity.⁵⁰ Air War Plans Division planners fully supported the plan despite the toned-down language from AWPDP 1 that advocated winning the war without an occupying force. The president’s objectives appeared to fall in line with the ACTS industrial web targeting theory.

Major Hansel believed that “the air offensive against selected targets [in AWPDP 42] should be vigorously pursued with full force for six months. The minimum effect should be a significant decline in operational effectiveness of the German army by the time the invasion of the European continent was

FROM AIRPOWER DEVELOPMENT TO TARGETING THE INDUSTRIAL WEB

ready for launching.”⁵¹ Tables 2.1 and 2.2 define initial targeting priorities of the Air War Plans Division with the intent of destroying the Germans’ will to fight and war-making capabilities.⁵² Table 2.1 projects priorities of targeting with required equipment and armament, whereas table 2.2 develops the number of targets for campaign planning.

Table 2.1. AWPDP 42 target priorities

First Priority: Destruction of the German air force (fighter factories, bomber factories, airplane engine plants)
Second Priority: Submarine building yards
Third Priority: Transportation (locomotive building shops, repair shops, marshaling yards, inland waterways)
Fourth Priority: Electric power (37 major plants)
Fifth Priority: Oil (23 plants)
Sixth Priority: Alumina
Seventh Priority: Rubber (two synthetic Buna plants)
Recapitulation: Targets: 177; Force required: 66,045 bomber sorties Bombs: 132,090 tons
Results: Decimation of the German air force; depletion of the German submarine force; disruption of German war economy

Reprinted from AWPDP 42, Requirements for Air Ascendancy, 1942 (Maxwell AFB, AL: Air Force Historical Research Agency [AFHRA], 1942), part 4, 3–4.

Table 2.2. AWPDP 42 target systems

System of Targets	No. of Targets	Percentage of Total Production Represented by Targets
Pursuit airplane assembly plants	11	100
Bomber airplane assembly plants	15	100
Aero engine plants; submarine yards	17	100
Submarine yards	20	100
Transportation	38	41.9 Locomotive building 31.5 Locomotive repair
Power	37	—
Oil	23	47
Alumina	14	100
Rubber	2	47.5
Total Number of Targets	177	

Reprinted from AWPDP 42, Requirements for Air Ascendancy, 1942, tab B-1-a, “Air Offensive—Europe” (Maxwell AFB, AL: AFHRA, 1942), 145.82–42.

Air war planning documents developed by the Air War Plans Division were a first for the Army Air Corps, later renamed the Army Air Forces in January 1942 by Secretary of War Henry L. Stimson. Note in table 2.1 how the targeting plan drove a required number of aircraft, 66,045 bombers to attack 177 targets; in other words, targeting drove an equipment requirement. It is evident that the US Department of War and President Roosevelt approved AWPD 1 and AWPD 42 plans, as evidenced both by Secretary Stimson's renaming of the Army Air Force and the air force's expansion to a "total of 115 groups, including 34 heavy bomber groups, 12 medium bomber groups, 10 light bomber groups, 31 pursuit groups, 12 transport groups, and 16 observation groups. This expansion was a step toward the goals established in AWPD 1."⁵³ The relevance of airpower was becoming pervasive.

Although it took some time for the Army Air Force to build a bomber force necessary to create the desired effects on identified targets, it was the plan for destroying identified targets that drove modest organizational change and equipping of the Air Force. It also drove the increase toward an initial 1.4-million-man draft force, as the United States postured itself for entry into the war. Aircrew training, initiated during prewar months and continued throughout the war, became extremely evident by the time US efforts transitioned from Europe to the Pacific. By late 1944 US pilots had undergone over two years of training.⁵⁴ These efforts were far different than US endeavors of organizing, training, and equipping an air force for action in World War I. Without the initial will of ACTS instructors to consider the possible effects of aerial targeting and their advocating for the opportunity to test these targeting theories, the senior civilian leadership may not have supported endeavors pursued in World War II.

The effectiveness and morality of area and precision bombing are continually debated.⁵⁵ Although not part of this treatise, scholars have written extensively about past wars and evaluated the effects of aerial targeting. The effectiveness and morality of targeting are relevant in any attempt to build a cyber-power targeting theory. These are necessary discussions that must occur in all realms of cyber warfare. From the planning to the postwar analysis of what worked and what did not, continuous improvements must occur.

Challenges to the Industrial Web Theory

Armchair quarterbacking frustrates the players as hindsight presents a clearer picture than looking into the unknown future does. This is akin to a historian writing about the past with an anticipation of changing the future.

Both are enjoyable because one can sit outside the sphere of execution and have the ability to analyze without the penalties or pain of reality and without responsibility. This is analogous to today's author writing about targeting theories of the past. The intent of the following is not to criticize or critique but rather to acknowledge additional considerations for future theorists of warfare targeting irrespective of the weapon system or warfare domain of choice.

Despite different airpower theorists who advocate the will of the people or war-making capabilities as strategic targets for ending war, each theory proposed finite objectives that gave the appearance of static confrontation or minimal adjustments by an adversary during warfare. An example of this thinking is seen by evaluating the tautology of the instructors at ACTS. After evaluating US cities, they concluded that destroying transportation, steel plants, ball-bearing manufacturers, food delivery systems, energy supplies, and especially electrical power facilities would disrupt vast economic systems and cause systemic disorganization.⁵⁶ Some of this rhetoric may be due to the belief that airpower was going to be so overwhelming that societies would capitulate once they witnessed the destructive power of being bombed from the air. In reality, the technology needed to create the desired effects did not exist until much later—during and after World War II. As enhanced long-range bombers, fighters, improved bombsights, navigational aids, and ultimately the atomic bomb came to fruition, so too did the ability to achieve the devastation airpower advocates thought possible.

When evaluating strategies for war, it is relevant to think about what is possible in each warfare domain; however, it is more practical to execute what is possible given the technology and training of the day in support of established doctrine. Lt Col Peter Faber highlights key questions any strategist of warfare, not just advocates of airpower, should ask.

- What facets of the opponent's power should we attack? Do we attack the *sources* (military, industrial, or cultural) of its power, the *manifestations* (governmental and ideological) of its power, or the *linkages* (human and material networks) that connect its resources?
- What targeting strategy should we use? Should we take a *direct* approach (head-on assaults), an *indirect* approach (maneuver warfare), or a *rapid transition* approach (observe-orient-decide-act [OODA] loop theory of adjusting pace with an opponent)?
- What level of destruction should we inflict? Do we want the physical or functional destruction of a particular target, or do we want to degrade a system's ability to operate, leading to victory?⁵⁷

The following is my interpretation of Faber's intended message regarding warfare. Some points Faber makes—for example, nations, not just militaries, fight wars—were previously known and articulated since the Napoleonic wars. However, if one focuses solely on targeting military entities within a nation to impose one's will on an adversary, one misses the interconnectedness not only of a nation's instruments of power but also of the people wielding each of those instruments. Next are the intangibles or immeasurable attributes of warfare such as culture or ideology and an examination of how a nation's people will react when threatened with the loss of beliefs or a way of life. Warfare is not a static constant. The enemy is a living, thinking, breathing entity with the ability to flex and change. To lose sight of this basic premise in war is to forgo the lesson of Sun Tzu, who stated, "know your enemy and know yourself."⁵⁸ Finally, before engaging in warfare, a nation's leaders should know the desired outcome and plans for achieving that outcome once victory in war is achieved. When possible, this is a critical point before war begins, as this knowledge directly contributes to determining a "total war" or "limited war" focus.⁵⁹ Recognizing the differences in these two ends of the spectrum of war is an ongoing challenge for political and military leaders. In reality, most wars will be fought somewhere between both ends. Therefore, militaries must decide which end they can organize, train, and equip toward in relation to assumed risks at the time.

A final thought relative to the industrial web and its seemingly specific targeting objectives centers on understanding expectations and capabilities as critical to effective strategy and planning for war and understanding the limitations of those expectations. It is also important to remember the need for flexibility and adaptability to changes in political objectives, as those changes have the ability to directly affect the conduct of war—both from allied and adversarial perspectives. When these changes occur, strategists must embrace new technology, tactics, techniques, procedures, and innovation to meet current and future challenges. Harnessing these opportunities and avoiding the notion of a single way to achieve success are vital in war planning and execution—just as they are during peacetime. There is no one path to success, and nothing is guaranteed to work as planned.

Summary

Table 2.3 highlights early airpower theorists and their prescribed target objective of airpower.⁶⁰ It is important to recognize that in airpower's infancy theorists subscribed to limited war-tested abilities and technological capabilities

and prescribed support of ground army actions as their postulated focus of both doctrine and targeting through 1945. The works of Douhet and Trenchard were known in the United States, if not directly then indirectly, through published articles and limited World War I experiences. Although Mitchell's contributions may not have directly influenced ACTS due to his court-martial, some men who served as ACTS instructors were his protégés from earlier career assignments. These men undoubtedly incorporated his vision into airpower doctrine. The result was a growing expectation of airpower and its effects in combat. Without debating the effectiveness of World War II bombing and the fact that the Army Air Force had more expectation than technical capability at the time, the targeting objectives espoused by the ACTS and the Air War Plans Division drove an air force capable of meeting wartime requirements. This was a first step toward airpower efficacy. All of these theorists and their actions drove initial and future OT&E functions of US air forces in some form—especially after World War II. This is discussed in the next chapter.

Table 2.3. Early airpower theorists and target objectives

Theorist(s)	Target(s)
Douhet	Population (cities)
Trenchard	War materiel, transportation, communications
Mitchell	Vital centers
de Seversky	All aspects of an industrial infrastructure
ACTS	Key economic nodes (war making materials, transportation, electricity, oil)

Reprinted from Lt Col Peter Faber, "Competing Theories of Airpower: A Language for Analysis" (paper presented at the Aerospace Power Doctrine Symposium, Maxwell AFB, AL, 30 April 1996).

Notes

1. Zhang, *Red Wings over the Yalu*, 13.
2. Douhet, *Command of the Air*. Douhet, an Italian airpower theorist, advocated the airplane as the offensive weapon par excellence and believed airplanes enabled a nation to completely destroy one's enemy while protecting one's own country. He is also credited with advocating for an independent air force. Although Douhet gained experience in World War I regarding the use of airpower, he is known for having less concern regarding moral bombing than other airpower theorists of the day. Douhet was focused on destroying the will of the people through physical destruction of a nation, once their air force was destroyed.
Britain's Hugh Trenchard was known as the father of the Royal Air Force and is credited as an early thinker regarding the concept of strategic bombing. A central element to his thinking was that strategic airpower offered an alternative to the "bloody, indecisive collisions along a

static front: the swift, deep, surgically precise stroke at just the right objective would ensure a rapid collapse.” Kennett, *First Air War*, 221. Finally, Trenchard pursued the offensive, accepted high casualties, and maintained a steady and unwavering determination to wear down the enemy through relentless attacks. He is known for taking and maintaining the offensive in the air in order to achieve moral as well as material dominance over the enemy. Wakelam, *Science of Bombing*, 5. In one of his famous quotes, Trenchard argued, “It is the deliberate opinion of those most competent to judge that . . . an aeroplane is an offensive and not a defensive weapon.” Biddle, *Rhetoric and Reality in Air Warfare*, 27.

Billy Mitchell is credited as the founding father of the US Air Force. In his book, Mitchell argued that “aviation must be developed for aviation’s sake and not as an auxiliary to other existing branches.” He said that to gain lasting victory in war, the hostile nation’s power to make war must be destroyed—this means the manufactories, means of communication, food production, farms, fuel and oil, and places where people live. When creating an aviation arm within a military, Mitchell argued for three distinct branches of an air force: pursuit aviation, bombardment aviation, and attack. Mitchell and Ehlers, *Winged Defense*, x, 127, and 164–71. It is asserted that Mitchell said civilian objectives would only be attacked “as an act of reprisal,” but in later years accorded greater importance to strategic bombardment, with an explicit emphasis on targeting vital industrial centers. Barlow, *Revolt of the Admirals*, 10.

3. International Committee of the Red Cross (ICRC), *Declaration (IV)*, 1).

4. Biddle, *Rhetoric and Reality in Air Warfare*, 181. See also ICRC, *Declaration (XIV)*. The United States and United Kingdom ratified this declaration, but France, Italy, Germany, and Russia did not. The declaration went into effect in 1909 and was supposed to be replaced at the Third Peace Conference; however, the conference never met, and some have argued that this declaration is still in effect.

5. Biddle, *Rhetoric and Reality in Air Warfare*, 19.

6. Kennett, *First Air War*, 17 and 42.

7. *Ibid.*, 43–44.

8. Joynson-Hicks, *Command of the Air*, 353.

9. Biddle, *Rhetoric and Reality in Air Warfare*, 25.

10. *Ibid.*, 26.

11. *Ibid.*, 27–29.

12. *Ibid.*, 49.

13. On 10 February 1908, Capt Chas. S. Wallace of the US Army Signal Corps entered into an agreement with the Wright Brothers to buy “one heavier-than-air flying machine, in accordance with Signal Corps Specifications No. 486, dated 23 December 1907.” The plane was to be delivered before 28 August 1908. Air Force Historical Research Center, “Signal Corps Specification, No. 486.”

14. Biddle, *Rhetoric and Reality in Air Warfare*, 49.

15. Hurley, *Billy Mitchell*, 2.

16. Gen John J. Pershing personally requested Gen Benjamin Foulois to assume the duties of chief of the Air Service, American Expeditionary Force in November 1917. General Foulois, however, recommended Billy Mitchell for the job of leading combat air efforts as chief of the Air Service, First Army. Shiner, *J.S.S. Foulois and the U.S. Army Air Corps*. Mitchell articulated his argument for aviation to become “a single department of aviation” throughout appearances before multiple congressional committees in 1919. Futrell, *Ideas, Concepts, Doctrine*, 32.

17. Finney, *History of the Air Corps Tactical School*, 4.

18. Raleigh and Jones, *War in the Air*, 213.

FROM AIRPOWER DEVELOPMENT TO TARGETING THE INDUSTRIAL WEB

19. Transcript of oral history interview with Foulois, as quoted in Kennett, *First Air War*, 41.
20. De Seversky, *Victory through Air Power*, 29.
21. See collection of Major General Hansell's military career from 1933 to 1955. USAF Historical Research Library, "Development of the U.S. Air Forces Philosophy," 1.
22. Finney, *History of the Air Corps Tactical School*, 7.
23. Ibid.
24. Ibid.
25. Mowbray, "Air Force Doctrine Problems," 2.
26. Ibid.
27. Finney, *History of the Air Corps Tactical School*, 63.
28. Ibid. *Zone of interior* refers to those areas of the theater of war that are outside the defined theater of operations.
29. Ibid., 65.
30. Ibid.
31. Ibid., 62.
32. Ibid., 63.
33. Ibid.
34. Ibid., 65.
35. Pape, *Bombing to Win*, 63.
36. Ibid., 65.
37. According to historian Campbell Craig, most American statesmen were quite content to limit US foreign policy. Craig, *Destroying the Village*, 2. These isolationist limitations came to an official end in 1949, when Secretary of State Dean Acheson completed negotiations for an Atlantic-region military alliance. The US Senate ratified the treaty on 21 July 1949, thus breaking the American isolationist tradition. Miller, *To Save a City*, 189–90.
38. Sherry, *Rise of American Airpower*, 47.
39. Ibid.
40. Ibid., 48 and 52.
41. Tooze, *Wages of Destruction*, 658.
42. De Seversky, *Victory through Air Power*, 123–52.
43. Tooze, *Wages of Destruction*, 402–4.
44. Biddle, *Rhetoric and Reality in Air Warfare*, 163–65.
45. See AWPDP 1, *Targeting for Victory*.
46. Ibid.
47. Ibid.
48. AWPDP 42, *Requirements for Air Ascendancy*, 1942.
49. Cody, "AWPD-42 to Instant Thunder," 13.
50. Arnold, memorandum.
51. Hansell, *Air Plan That Defeated Hitler*, 85.
52. Cody, "AWPD-42 to Instant Thunder," 17.
53. AWPDP 1, *Targeting for Victory*.
54. Peattie, *Sunburst*, 187.
55. However postwar analysis is described, Britain and the United States started the war with independent air operations against an enemy's material and moral resources. For Britain, air attacks were aimed at the sources of an enemy's strength in order to restore decisiveness to warfare and to produce a much swifter and more humane decision. As for the United States, targeting the enemy's industrial web was the focus of strategic bombers, as derived from ACTS.

FROM AIRPOWER DEVELOPMENT TO TARGETING THE INDUSTRIAL WEB

Following the war, many writers criticized the strategic air campaigns against Germany and Japan; some even claimed force was employed “beyond reason.” Much of the controversy centered on the ineffectiveness and inhumanity of RAF Bomber Command’s avowed policy of area bombing directed against German civilian morale and around the long-delayed effectiveness of US precision bombing efforts and the drift of US attacks towards a bombing of more “clublike than swordlike.” Additionally, questions were posed as to whether the immense material and human efforts devoted to bombing campaigns might have been more useful elsewhere. Paret, Craig, and Gilbert, *Makers of Modern Strategy*, 633–37.

56. Quoted in Sherry, *Rise of American Airpower*, 54.

57. Faber, “Competing Theories of Airpower.”

58. Sun Tzu, *Illustrated Art of War*, 125.

59. Limited war refers to wars fought with “limited means for limited objectives.” Paret, Craig, and Gilbert, *Makers of Modern Strategy*, 94. Total war is explained succinctly by Clausewitz when he says, “if you want to overcome your enemy you must match the total means at his disposal and the strength of his will.” Clausewitz, *On War*, 77. Mobilizing a nation’s full resources and society to conduct warfare against an adversary is total war.

60. This target set is a compilation of reference material reviewed in Faber, “Competing Theories of Airpower.”

Chapter 3

Targeting

From Industrial Web to Warden's Rings

The key to airpower is targeting and the key to targeting is intelligence.

—John A. Warden III
The Air Campaign

In *The Rise of American Airpower*, Michael Sherry quotes Hap Arnold: airpower's purpose is "to destroy our targets."¹ Although an oversimplification of American airpower capabilities in World War II, Arnold's comment highlights the strategic-level thinking and overarching military objective of early airpower advocates. One of Sherry's themes throughout his book is that early airpower leadership failed to view aerial weapons as instruments of war that kill and destroy; it is this lack of understanding which contributed to the growth of and advocacy for aerial weapons.² But was Sherry correct in his observation of airpower advocates?

This chapter disputes Sherry's claim by highlighting a contemporary airpower theorist who not only experienced aerial weapons that kill and destroy, but also created an air campaign strategy to conduct airpower operations with great efficiency for killing and destruction. Sticking with my focus on targeting, the objective of this review is to recognize how the air campaign planning strategies of Col John A. Warden III furthered airpower efficacy while evaluating his theory for use in cyber power targeting. Specifically, how did Warden's principles aid airpower in becoming a decisive instrument of power? Did Warden build on targeting principals of ACTS or develop a new targeting theory? Is there a parallel between Air Force OT&E functions and Warden's centers of gravity systems approach—the five-ring model?

Airpower Targeting Evolution: Post World War II

The Korean and Vietnam Wars are the most well-known US wars after World War II. The Cold War is another well-known war where actual combat between Soviet and American forces did not occur directly, although the Korean and Vietnam Wars are linked to the US containment policy of the Cold War, and the Soviets supported adversaries of the United States on both occasions.

TARGETING

The use of airpower conjures several questions regarding airpower targeting strategies used in both conflicts. How did airpower targeting strategy influence operations in the Korean and Vietnam Wars? How did these two wars influence the airpower targeting strategy used in Operation Desert Storm in 1991? The first portion of this chapter lays the foundation for airpower's use.

Korean War

Despite airpower limitations evidenced in World War II by the lack of precision bombing and limited technology in navigation, radar, and weaponry, Americans entered the Korean War with inflated expectations of what airpower could accomplish.³ Perceptions regarding airpower limitations may have been negated by advancements in airpower technology during World War II, which culminated in the most advanced air weapon ever made—the atomic bomb. However, the US Air Force entered the Korean War using the same targeting theory developed in the 1920s. Airmen hoped to achieve air superiority and gain victory by bombing economic and military targets to eliminate the enemy's capacity and will to wage war.⁴

Airpower doctrine and teaching of the day did not evolve beyond the teachings of ACTS. Maj Gen Orville Anderson, commandant of the Air War College in 1949, confirmed the unchanged targeting strategy. "The strategic objective of airpower is the elimination or reduction of the enemy's power and power potential. The target may be selected segments of his industrial establishment, his communications or transportation system, the source of his governmental or social control, or his military forces in being," he said.⁵ These teachings failed to capture the actual use of aerial warfare in the European and Pacific campaigns of World War II. Morale bombings, which were not a part of the industrial web theory, were employed in each theater to achieve combat objectives. The teachings also did not advocate for simultaneous targeting of defined centers of gravity.

In early February 1945 the first major American morale bombing raid in Europe was Operation Thunderclap, which was intended to destroy Berlin and influence its citizens to surrender.⁶ In 1945 the American bombing campaign in the Pacific shifted from interdiction to attacking civilian morale through incendiary raids on urban areas.⁷ Despite differing opinions about the effectiveness of morale bombing, these actions showed that the United States was willing to go beyond aerial targets of the industrial web theory to achieve military objectives. Robert Pape made this point when he said, "Western publics have shrunk from using indiscriminate means against noncombatants to

pressure other states.”⁸ However, following World War II, there is little evidence that aerial bombing focused on degrading enemy morale became part of Air Force doctrine. This is undoubtedly due to the stigma of immorality attached to directly bombing civilians.

Countering published airpower doctrine for strategic bombing, in 1949 Bernard Brodie advocated for the targeting of civilian morale. Brodie argued, after studying the United States Strategic Bombing Survey report, *The Effects of Bombing on German Morale*, that devastating attacks at a highly concentrated time could cause depressed enemy morale.⁹ This was not a new concept. Early airpower zealot Giulio Douhet argued that once command of the air was achieved, air forces should keep up violent, uninterrupted action against surface objects, so that the material and moral resistance of the enemy may be crushed.¹⁰ Douhet posited that a battlefield will be limited only by the boundaries of nations at war, and all of their citizens will become combatants; there will be no distinction between soldiers and civilians.¹¹

What airpower strategists must remember when advocating Douhet’s, as well as Brodie’s, principles for targeting is that political boundaries will limit airpower, or any military objective for that matter, more than doctrine or military capabilities of the day. This is especially true in limited wars such as Korea. Xiaoming Zhang succinctly captured this point at the end of aerial conflict in the Korean War. “The air war came not to a military conclusion, but a political one. The American strategy of using aerial bombardment achieved few political or military goals despite the initial belief of many in Washington that airpower alone could defeat the enemy in Korea,” he said.¹² For this reason, military strategists must consider all potential targets and their prohibitions during warfare in order to avoid constraints while enabling airpower to achieve stated and fleeting objectives. Even if the United States is prohibited from prosecuting some targets due to moral constraints, the adversary may not be constrained by the same principles. As such, thinking about the full range of potential offensive targets will highlight enemy force vulnerabilities while defining objectives for defense operations.

Between the Korean War and the next limited war in Vietnam, which was also constrained within the context of containing communism, US civilian leadership pursued a strategy informed by the airpower targeting doctrine of the day. Although focused on nuclear targeting, the “no-cities” doctrine espoused by then-secretary of defense Robert McNamara highlights the US moral concern of not targeting cities directly with airpower.¹³ McNamara was searching for a flexible nuclear response in warfare as an alternative to “Eisenhower’s all or nothing military policy” of the day.¹⁴ This counterargument does not diminish the objective of minimizing casualties and damage caused by airpower to

TARGETING

those forces either making war or directly supporting the war effort. The principles of controlling, restraining, and manipulating war apply to both conventional and nuclear force application in all military domains and must be considered in the newest war-fighting domain of cyber as well.

Vietnam War

Political agendas and the fear of war escalation constrained airpower objectives during the Vietnam War. These constraints inhibited airpower from executing targeting doctrine by restraining military operations from attacking vital centers supporting war-making efforts, especially early in the war. Geography drove target selection; almost all targets picked before August 1965 were south of the 20th parallel.¹⁵ Pres. Lyndon B. Johnson's personal control of the air war, evidenced by his approving target lists at the Tuesday White House luncheons, limited options for air commanders.¹⁶ North Vietnamese cities, airfields, and surface-to-air missile sites under construction became "prohibited areas" for air attacks to avoid provoking the Russians and Chinese to enter the war.¹⁷ Constraints imposed on air planners drove target selection based on three objectives: the value of a target, the risk to US pilots, and the risk of widening the war.¹⁸

Airpower constraints waned as Johnson began to see the air campaign as a means to bring the North Vietnamese to the negotiating table. From the beginning of the conflict, Airmen advocated a four-phase (table 3.1) 94-target (table 3.2) plan focused on transportation systems, oil storage facilities, and other industrial components they perceived as vital to the northern war effort.¹⁹ After the Tet offensive in January 1968, Johnson not only removed target restrictions from cities like Hanoi, but also supported the commanding general who pressed for approval to strike targets that "might produce civilian casualties."²⁰ The Tet offensive caused air leaders to diverge from their doctrinal convictions that industrial targets were the proper objectives in Vietnam. Military historian Mark Clodfelter argued that political and military controls prevented attacks against the only two targets that would have affected northern war-making capacity: people and food.²¹ The loosening of these controls freed airpower application to move beyond the industrial web targeting theory of the day.

Table 3.1. JCS four-phase air campaign proposal

Phases	Targets	Objectives
One (3 weeks)	Lines of communication (LOC) below the 20th parallel	Reduce the flow of logistics by battering the LOCs with almost continuous attacks, and provide a clear indication to the North Vietnamese that we would increase the scope and intensity of the war if they continued their efforts to overthrow the government of South Vietnam.
Two (6 weeks)	Northeast and northwest railroads to China	Cutting these rail lines would hit the logistical system at its most vulnerable points and would bring the war closer to the people and the government, thereby attacking both the means and the will of the North Vietnamese to fight.
Three (2 weeks)	Ports, mine seaward approaches, ammunition, and supply areas in the Hanoi-Haiphong area	The United States would expect the North Vietnamese to decide that South Vietnam was no longer worth the price. By the end of phase three, most of the targets on the 94-target list would have been struck.
Four (2 weeks)	Industrial targets outside populated areas	The intent was to hit any earlier targets that had not been fully destroyed or had been repaired.
The president and secretary of defense elected only to increase the pressure on LOCs below the 20th parallel.		

Adapted from William W. Momyer, Airpower in Three Wars (Washington, DC: Department of the Air Force, 1978), 19.

Table 3.2. JCS 94-target scheme

Airfields
Lines of Communication
Military Installations
Industrial Installations
Armed Reconnaissance Routes
Results: End the war by employing airpower intensively against strategic targets in North Vietnam through a concentrated strategic air offensive.

Reprinted from Robert Frank Futrell, Ideas, Concepts, Doctrine, vol. 2, Basic Thinking in the United States Air Force, 1961–1984 (Maxwell AFB, AL: Air University Press, 1989), 259.

During Richard Nixon's presidency, the United States lost a basic necessity for a nation at war: public support. A South Vietnam spoiling operation against the Communists known as Lam Son 719 convinced the American people that "sacrifices on behalf of South Vietnamese were no longer warranted."²² However, shortly after taking office Nixon assured the nation that he

TARGETING

would do whatever was necessary to safeguard American lives and honor while not abandoning the South Vietnamese.²³ Nixon expanded the military target objectives by allowing aircraft to mine northern ports and interdict lines of communication (Linebacker I and II). His intent was to press the Communists until the northern leaders agreed to release American prisoners and support an internationally supervised cease-fire.²⁴ Nixon's clearly defined political objectives enabled air chiefs to execute Linebacker operations with three simply stated objectives: (a) destroy war material in North Vietnam; (b) prevent the flow of war material in Vietnam; and (c) interdict the flow of troops and material from the north into combat areas, South Vietnam, Laos, and Cambodia.²⁵

In addition to clearly stated presidential directives, the success of Linebacker operations came from the Communists' change from guerilla to more conventional tactics, which suited the Air Force bombing doctrine of the day. Tanks and heavy artillery, as well as logistic transports intended to resupply enemy forces, were effectively targeted and destroyed during the North's eastern offensive. The delegated authority to the air chiefs to attack various targets simultaneously while controlling air operations with a single commander contributed to the success of air operations in 1972, which encouraged Communist concessions; both are required lessons for successful future air operations.²⁶ These changes are evident in the post-World War I airpower theories espoused in chapter 2. Specifically, there is a "focus [of] air attacks on enemy rear positions" and placing airpower "under a single commander."²⁷

Reviewing the Wars

Differences between World War II and the Korean and Vietnam Wars can be attributed to "total" versus "limited" war objectives. In World War II, the objectives of unconditional surrender were the mandate. In both the Korean and Vietnam Wars, US politicians' fear of escalation governed war actions. The United States did not want to draw the Soviets into a prolonged war. Thus limited military objectives with political restrictions and prescribed rules of engagement were the order of the day. Political restrictions aside—and despite some technological innovations between World War II and the Vietnam War such as long-range bombers, radar, target navigation systems, jet fighter aircraft, precision weapons, upgraded electronic warfare, and antiradiation missiles—the Air Force and political leadership failed to learn the lesson that air bombardment alone, as prescribed by the industrial war objectives, could not win a war.²⁸

Attacking industrial web targets along with economic, civilian, and politically sensitive targets simultaneously and continuously, without day-to-day targeting control by civilian leadership, is required for effective airpower. Both Korea and Vietnam showed that limited war is different than total war; adversaries fighting a guerrilla campaign in a limited war are largely immune to conventional air attacks.²⁹ It is difficult to identify, target, and destroy the dispersed industrial web of a guerrilla force. Therefore, limited wars require a different way of thinking about warfare and strategies regarding military target objectives. Col John A. Warden III, a veteran Vietnam pilot, is one such thinker. He spent his career developing a contemporary targeting theory for airpower and proved its use in the limited war of Operation Desert Storm in 1991.

The Making of a Strategist

It can be argued that the advent of nuclear weapons, at least at the operational and strategic levels of war, caused a lack of critical thinking about targeting with airpower. Given the destructive power of nuclear weapons, arguments for less precision bombing are viable. However, the destructive power of nuclear weapons did not abate Air Force leaders' advocacy for precision strategic bombing articulated by ACTS in the 1930s. Combat in World War II showed that the bombers did not always get through, at least not without fighter escorts in highly contested environments. Neither Korea nor Vietnam changed airpower advocates' beliefs "about the unprecedented decisiveness of well-targeted, well-executed bombardment attacks."³⁰ A derivative of this line of thinking—between the 1930s and 1990 when Iraq invaded Kuwait—was the focus on tactical airpower as evidenced by the rise of the Tactical Air Command and the future post-Vietnam Air Force generals. Warden came along and thought that the Air Force needed to think more about strategic warfare as being *the* dominant form of warfare.³¹

According to Colonel Warden, airpower is constrained only by the limits placed upon it.³² Warden developed these views from his 266 combat missions flown in Vietnam, and his own studies of warfare. He espoused that there is no such thing as limited war, and victory could never be gained by constant cycles of concessions and escalation.³³ Although there were constant perceptions that concessions and escalations, along with rules of engagement, existed in Vietnam, civilian leadership dictated limitations daily.

Warden's experiences and training led him to believe that airpower was most effective when used as an offensive and aggressive weapon and that good tactics could not compensate for a flawed strategy.³⁴ Warden's interest in

flawed strategies led him to think about the strategic and operational levels of war while working at the Air Staff. His interests culminated in academic studies at Texas Tech, where he initiated personal studies on grand strategy, which led to his thesis, “The Grand Alliance: Strategy and Decision.”³⁵ It was during this time that Warden came to believe that a strategist should think in terms of paralyzing, not of killing, and should not consider the army as the only focus to achieve victory.³⁶ These views can be seen in a book Warden authored while at the National War College, *The Air Campaign: Planning for Combat*. Although Warden argues for three types of combat missions—air superiority, interdiction, and close air support—we begin to see Warden’s targeting theory for air forces in his book.

Developing an Air Campaign and New Targeting Theory

In developing a strategy for air campaign planners, Warden articulates that military objectives will vary and militaries must understand these variances to properly affect military objectives. He said military objectives tend to fall into three general categories. First, the military objective can be the destruction of some or all of the enemy’s forces. The importance of political objectives, as viewed by the enemy, will determine the degree of destruction of enemy forces necessary by allied forces.³⁷ Second, the military objective can be the destruction of some or all of the enemy’s economy, especially war-related economy.³⁸ Third, the military objective can be either the will of the government or the will of the people.³⁹ Despite historical conjectures that “a nation is not conquered until the hearts of its women are on the ground . . . no matter how brave its warriors nor how strong its weapons,” this last objective is the most capricious of all military objectives.⁴⁰ The will of a people is the most difficult to define, observe, and measure in terms of military effectiveness. With the objectives defined, Warden transitioned to what this author deems is the most critical aspect of any targeting strategy, a focus on centers of gravity.

Enemy centers of gravity can be equipment (number of planes or missiles), logistics (the quantity and resilience of support), geography (location and number of operational support facilities), personnel (numbers and quality of pilots), or command and control (importance and vulnerability).⁴¹ Warden’s early thinking on centers of gravity is focused on airpower objectives, but he clearly believed the commander’s most important task was identifying the centers of gravity correctly and striking them appropriately.⁴² His thinking mirrors those of Clausewitz, who said that “identifying the centers of gravity is the first task in planning for war.”⁴³ To reiterate, identifying centers of gravity

that will drive military targeting objectives is applicable to all war-fighting domains—including cyber.

Warden posits that “targeting priorities will be a function of perceived enemy air centers of gravity.”⁴⁴ This statement can be restated as “centers of gravity determine the targeting priorities for military forces no matter the domain from which an offense is conducted.” A review of World War II operations makes Warden’s point for both the Pacific and European theaters. While focused on Axis power targets in Europe, intelligence information showed German ball bearing factories as choke points to military weapon manufacturing; therefore the United States targeted the factories with airpower. From an Allied perspective in the Pacific, General Hansell recognized a need to have bases within 1,600 miles of Japan to attack there. This made seizing bases in the Marianas a center of gravity for the United States.⁴⁵ It is from his historical studies of centers of gravity that Warden developed what has become his “five-ring” model.

By 1988 Warden perfected his strategic thinking in an essay called “Global Strategy Outline.” In it he portrayed the enemy as a system with certain centers of gravity which, when affected by airpower, would cause an adversary to concede due to the heavy cost of continuing a war.⁴⁶ Different versions of Warden’s five “strategic rings” model exist, but the elements remain constant although updated from his earlier thinking. Table 3.3 and figure 3.1 depict Warden’s theory.⁴⁷

Table 3.3. Warden’s five-ring model with objectives

	Target	Objective
Inner Ring	Command & Control / Leadership	Destroy the enemy’s command and control from the highest civil command to appropriate level of military command
Second Ring	War Materials	Destroy enough of the enemy’s war material base that he is unable to support fielded forces
Third Ring	Infrastructure	Destroy or damage enough infrastructure so that movement of goods and services becomes impossible
Fourth Ring	Population	Impose sufficient hardship on the population that the people become either unwilling or unable to support the war effort
Outer Ring	Fielded Forces	Destroy or incapacitate enough fielded forces that the enemy is unable or unwilling to continue effective offensive or defensive operations

Adapted from John A. Olsen, John Warden and the Renaissance of American Airpower (Dulles, VA: Potomac Books Inc., 2007), 149.1p0.

TARGETING

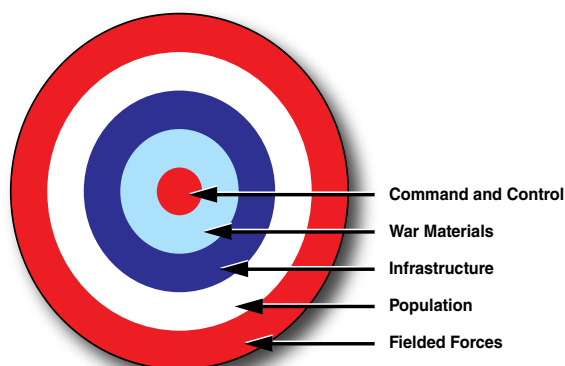


Figure 3.1. Warden's five rings. (Adapted from John A. Olsen, *John Warden and the Renaissance of American Airpower* [Dulles, VA: Potomac Books Inc., 2007], 149.)

Understanding the importance of a center of gravity is nothing new in warfare. During the Peloponnesian War in 431 BCE, Sparta recognized Agamemnon's Athenian navy as the strongest in the region and thus a center of gravity, just as Athens viewed Sparta's military power in the Hellas as its center of gravity.⁴⁸ Another center of gravity during the Peloponnesian War is succinctly identified by Pericles during his speech at an Athenian assembly where he encouraged Athens not to give in to Sparta's requests. Pericles identified Athenian allies as a source of power. He argued that if Athens did not march against Sparta, Athens would surely lose them.⁴⁹ Just as today, military strategies more than 2,400 years ago had to understand and identify centers of gravity before determining ways to influence or destroy them in warfare.

Warden understood the history of warfare and knew he was not advocating a new principle. He created a modeling tool that included both the mechanical and social aspects of a system.⁵⁰ In a mechanical analysis of his system, Warden evaluated the Soviet fuel storage capacity, something the intelligence community did not deem a center of gravity. Warden tested his center of gravity theory and determined that if the United States and its allies destroyed *how* Soviet fuel was transported, and not *where* it was stored, the Soviets would run out of fuel in three to five days.⁵¹ This changed the perspective of air planners, who had concluded previously that the Soviets would have six months of fuel storage in bunkers that could not be effectively destroyed. Warden's theory demonstrated that evaluating the entire system of a capability made it irrelevant to target every aspect of that system and ultimately reduced the effort required to affect the system.

Warden's model, as he postulates, is used for more than military application. For the purpose of this study, the model portrays a targeting theory bounded by an understanding that enemy systems are integrated and reliant upon one another. It is also based on a notion that each objective has a center of gravity that supports the adversary's war-making ability. In defining general targeting objectives, Warden's model focuses military attention on strategic areas required for effective air campaign plan development. This same focus applies to all war-fighting domains: land, sea, air, space, and cyber.

Advancing a Targeting Model

Before evaluating the difference between the ACTS targeting theory and Warden's five rings, there is an amendment one could make to his model. A sixth ring could be added, placed between the first and second, pushing the remaining elements out one level. The new second ring would be labeled *intelligence*, with an objective of either destroying or disrupting the intelligence gathering capabilities of the adversary, or influencing an enemy's intelligence with information operations. This would deceive the enemy regarding friendly intentions, capabilities, and actions.

As the opening quote of this chapter suggests—and given the reliance on accurate intelligence for decisions regarding war and execution throughout war—intelligence is a center of gravity for any nation or entity in peacetime and war. The intent is not necessarily to target intelligence briefs used by leadership for decision making; that would be futile. However, if key processing centers that collect, analyze, and synthesize the data are determined, those key nodes would be centers of gravity for a critical resource—intelligence.

Clausewitz acknowledged that “intelligence reports in war are contradictory; even more are false, and most are uncertain.”⁵² He said that the difficulty of gaining “accurate recognition constitutes one of the most serious sources of friction in war.”⁵³ His point should not be lost on military strategists or war planners. A nation that creates unreliability or uncertainty in intelligence creates friction for the adversary. It also creates an advantage to the one causing the disruption, as long as its intelligence is protected from the same effects. For this reason, I argue *intelligence* is a center of gravity and is part of any strategic tool used in modeling combat operations.

While finalizing an updated enemy-as-a-system targeting model, I was graciously afforded a 90-minute interview with Colonel Warden, who agrees with my position. In discussing what enhancements might be made to the targeting model, Colonel Warden advised that the second ring has undergone

TARGETING

multiple iterations to capture his true intent and vision from a strategic perspective. From “key production” to “system essentials” to “organic essentials,” the name did not clearly capture Warden’s intent. Finally, after years of continued education, refinement, and feedback, Warden updated his enemy as a system model by calling the second targeting ring “key processes.”⁵⁴ This change succinctly captures varying elements leadership requires to conduct warfare, including my concern for key intelligence collection, processing, and distribution centers. With Colonel Warden’s approval, the updated model is referenced in figure 3.2.

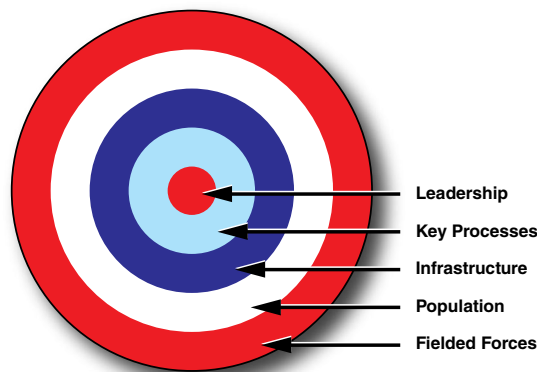


Figure 3.2. Warden’s updated rings. *(Created by author based on interview with Col John Warden.)*

Strategic Targeting: Moving beyond ACTS

Colonel Warden depicted the success of his systems targeting model when he said that “fail[ing] to understand the shift from the physical to the function[al] obfuscate[s] analysis.”⁵⁵ It also obscures strategic thinking. As strategists develop a theory, there must be a way to convey the theory for application; otherwise it is just a theoretical dream. As everyone knows, nightmares are dreams too. Without further digression, following through on developing a theory requires analysis once it has been applied to determine the effectiveness of the theory. The more analyzed and enduring the theory, the more widely accepted and used it becomes—at least until another revolution occurs to change the paradigm.⁵⁶

Some pundits argue Warden's theory was simply an update to "theories developed at the ACTS," as is suggested in an *Airpower Journal* article.⁵⁷ I disagree. Warden's additions to the theory of airpower and its efficacy went beyond terminology and labels such as "vital centers." Warden drove the focus of strategic thinkers from the tactical-level effects of airpower up toward the operational- and strategic-level effects of airpower. Yes, both ACTS and Warden espoused targets as part of a system. Both appeared to understand the interrelation of systems when talking about specific functions such as railways providing logistics or communications systems providing command and control. But it was Warden's targeting model that highlighted how attacking disparate centers of gravity—in a simultaneous/parallel manner and not a serial/escalatory manner—creates synergistic effects upon the enemy. It was this model that enabled Airmen to show how strategic objectives could be achieved with airpower, as Warden did to the secretary of defense during Desert Storm.⁵⁸

Since Warden was a literary student of Clausewitz, it is only fitting that his comparison to the studies and theories of ACTS be equated to Clausewitz and his studies of the principles of war.⁵⁹ Military strategists agree that Clausewitz was not the first to articulate or use principles of war in battle, as evidenced during the Peloponnesian War. Although a center of gravity is not a principle of war, defining an objective, massing forces, and using economy of force, speed, surprise, and others to affect a center of gravity are critical to success in combat. Therefore, early practitioners of the military art of war must have understood the principles of war, even if they were expressed with different terminology. This is exactly how Warden is compared to Clausewitz.

Clausewitz, in *On War*, is credited with combining the principles of war in a manner practitioners of war could understand and apply, as demonstrated by his popularity in the curricula of military and civilian education systems around the world. Clausewitz's combination of the separate principles of war was written showing how synergistic effects could be created by carefully planned and executed actions in war—actions which could overwhelm an adversary and cause capitulation. It highlighted the interconnectedness of the systems used in warfare and why military tacticians and strategists should look at the enemy with a holistic approach to determine capabilities, vulnerabilities, and limitations.

On War also provides military leaders with a valuable textbook for potential success in combat, although that is presumably not what Clausewitz intended since there are no guarantees in war and the "result is never final."⁶⁰ This is precisely what Warden did; he studied the art of war, applied technical capabilities of the day, and built a targeting model based on the systems approach of the enemy centers of gravity. His model also represents a tool which can be used to

TARGETING

plan air campaigns—and arguably a campaign in any war-fighting domain—focused on achieving strategic effects in war. Finally, Warden cemented the breakaway from military doctrine ACTS could not accomplish.

Although the Air Force became a separate service in 1947, there was not a war where airpower demonstrated its efficacy as it did in Desert Storm. Military doctrine during the ACTS era stated that airpower provided a supporting and secondary role to ground forces as soon as air superiority was achieved.⁶¹ Warden's advocacy showed air can perform the dominant role in combat and do it with precision. His theory's focus was designed to incapacitate the leadership and achieve functional disruption and strategic effects, rather than focus on physical destruction exhibited by strategic bombing in World War II. In essence, Warden's theory went beyond what ACTS developed in thinking, understanding, and action. The case study below supports this claim.

Case Study: The Enemy as a System (Five-Ring) Targeting Schema

On 8 August 1990 Gen Norman Schwarzkopf phoned the Air Staff asking for a targeting plan in case Saddam Hussein committed some “heinous” act.⁶² This was a preemptive action by the Central Command (CENTCOM) commander as there were no presidential directives for action against Iraq at this point. It put the wheels in motion for what some consider a “new era of warfare.”⁶³

Timing is everything. As the deputy director for war-fighting concepts, Colonel Warden had already begun to look at a “strategic” set of targets for Iraq.⁶⁴ Through analysis of how best to apply airpower in an independent fashion and a self-directed investigation of how his core set of ideas could be applied to Iraq, Warden and his team were able to present an air campaign against Iraq the same day they received the request.⁶⁵ Built on assumptions that the United States would act without substantial allied support and that weapons used would cause selective damage, unlike the mass aerial bombings of World War II, the air campaign was designed to limit American losses, Iraqi civilian casualties, and collateral damage.⁶⁶ There is no doubt Warden shaped these assumptions based on his knowledge of the history of warfare, as well as his own experiences in Vietnam.

Warden presented a plan based on political objectives derived from the president's speeches, press conferences, and newspaper articles.⁶⁷ All objectives (table 3.4) were intended to be accomplished within six to nine days of executing the air campaign. As the table shows, the objectives Warden and his team developed for the initial air campaign plan look extensively like Warden's

model in figure 3.2. This example not only shows Warden's belief in his model, but highlights the influence his position on the Air Staff afforded him in influencing senior airpower decision makers.

Table 3.4. Initial Gulf War objectives

Strategic Target	Linked to Warden's Ring	Campaign Target Objective
Leadership	Inner Ring	Two target sets: Hussein regime (isolate & incapacitate), and communications (both civil telecommunications and military command, control, and communications)
Key Production	War Materials	Four target sets: electricity, oil distribution and storage facilities, one nuclear, biological, and chemical research facility in Bagdad, and military production and storage facilities, including SCUD-related targets
Infrastructure	Infrastructure	Railroads as a target set with one railway and highway bridge as a subset
Population	Population	Three target sets: Iraqis, foreign workers, and soldiers in Kuwait (these targets were to be struck with only non-lethal, psychological weapons)
Iraqi Fielded Military Force	Fielded Forces	Two target sets: Iraqi strategic air defense system and the Iraqi strategic offensive system (bombers & missiles). The Iraqi Army was not a target set originally.

Reprinted from Diane T. Putney, "From Instant Thunder to Desert Storm: Developing the Gulf War Air Campaign's Phases," Air Power History 41, no. 3 (Fall 1994): 41.

Warden briefed the Instant Thunder plan to General Schwarzkopf on 10 August 1990. Schwarzkopf later recalled, "I felt a hell of a lot better after I left the briefing room than when I entered it. Warden turned on the proverbial light bulb."⁶⁸ In name alone, Instant Thunder portrayed a departure from the failed Rolling Thunder of Vietnam.⁶⁹ Warden's team developed a plan intended to be quick, overwhelming, and decisive, exactly the type of "retaliation plan" the general sought.⁷⁰

After receiving input like Gen Colin Powell's "not being happy until he saw tanks destroyed" and other inputs received during planning briefs, Warden's team developed Instant Thunder Phase II.⁷¹ The target sets continued to increase as airfield and naval ports were added. Before the plan was briefed to Lt Gen Charles Horner, the commander of US Central Command Air Forces in Saudi Arabia, only 84 targets existed on the list. Once General Horner's team took over air campaign planning, the target list grew to 481 by early January as

TARGETING

honed intelligence—something precrisis planning showed as deficient—became available.⁷² Warden's targeting strategy was now in motion.

On 16 January 1991, when Baghdad went "black" 45 seconds into the war, Warden proclaimed, "The war is over, we won."⁷³ Although the air war lasted longer than the six to nine days originally estimated, and despite all the convincing Warden had to do at the highest levels of the DOD to allow the air war to continue beyond those initial estimates, Warden's strategic targeting model proved accurate in the end, despite a 100-hour ground campaign by the US Army.⁷⁴

Evaluating Success

The Gulf War Air Power Survey captures the effects of Warden's targeting model in the opening sentence of its more than 400 detailed pages: "In many ways 'Desert Storm' represents a watershed in history; for much of the war, it consisted entirely of the application of massive doses of airpower to the economic and bureaucratic infrastructure of Iraq and its military forces."⁷⁵ Instant Thunder provided mass, enabled air superiority through speed and surprise, and, as the airpower survey states, "compared to previous wars, the bombing of core strategic targets in Iraq was remarkably precise and discriminate."⁷⁶ After more than 40 years of unfulfilled promises, airpower achieved the concept of "victory through airpower" that Giulio Douhet, Billy Mitchell, and Hugh Trenchard espoused.⁷⁷ In developing a systems targeting model that enabled victory through airpower, Warden truly measures up as one of the prevailing contemporary airpower theorists. Therefore, it is relevant to evaluate whether Warden's five-ring model changed the Air Force OT&E functions in any way.

Organizing, Training, and Equipping to a Contemporary Targeting Model

Desert Storm was unlike World War II in that the United States did not have years to plan for equipping, training, and organizing forces before entering combat. Desert Storm happened within months of Iraq's invasion of Kuwait in August 1990; therefore, the Air Force went to war with the force it had.⁷⁸ Given this perspective and the fact that Warden's model was literally developed just months before the Gulf War, the only logical review of any OT&E changes is to observe improvements since the Gulf War. I postulate that a detailed evaluation of Air Force OT&E functions post Gulf War will highlight whether Warden's model truly influenced changes in each functional area. This will make a great future study by other academics. For now, I provide a brief

evaluation of perceived major changes from previous wars that enabled air-power success in Desert Storm and describe perceived influences on future OT&E functions.

The Gulf War Air Power Survey reported that one of the crucial differences regarding organization during the conduct of the air campaign against Iraq, compared to Rolling Thunder in Vietnam, is the use of *one* individual responsible for the conduct of the campaign.⁷⁹ General Horner served as the JFACC and controlled interservice and coalition air forces. As the JFACC, Horner focused the air campaign on objectives originally defined by Warden. He seized the initiative by attacking, isolating, and incapacitating the Iraqi military leadership and destroying Iraq's ability to conduct military operations.⁸⁰

With a single air component commander, the management of tactical to strategic military objectives is better controlled than when multiple decision makers are involved, especially in time-sensitive environments. Competing interests over service-specific objectives or priorities were vetted, but in the end, there was only one decision maker with airpower authority, and it proved successful. The fact that joint air force operations occur today with a single air component commander proves that airpower operations achieve maximum efficiency and effectiveness when a single air component commander is in charge of airpower operations.

Inefficiency existed during the Gulf War which training could have prevented. Under the actual conditions and pressures of war, human systems and organizations rarely work at optimal levels, especially at the beginning.⁸¹ The pace of operations and the flow of intelligence created a challenge by the third day of Desert Storm, as the first two preplanned days of air operations morphed into daily planning requirements for the air tasking order and master attack plan. As the Gulf War Air Power Survey shows, the complexities involved in the daily planning cycle were not clear before the war.⁸² A 300 percent increase in cancelled operations after day two of the air campaign highlighted the coordination failures. It took approximately a week before satisfactory coordination occurred and operation cancellations decreased.

Peacetime training to generate air tasking orders and coordinate master attack plans, as the operating tempo demanded in the early days of the Gulf War, presumably did not exist. At the highest monthly rate in Vietnam, 4,000 sorties were flown each month. It is safe to proclaim that joint and coalition forces had not experienced, nor trained to, that level of air tempo in the past four decades when compared to the approximately 100,000 sorties flown in the five-week Gulf War.⁸³ However, this is exactly the tempo principles of war dictate. As for the number of sorties generated in such a short duration, a large force is what enables Warden's five-ring parallel targeting system.

TARGETING

Without mass, simultaneous operations cannot occur, and escalation of airpower is an operational consequence, which is like stepping back to Vietnam operations. To prevent disorder and aid future air operations, the Air Force conducts air tasking order plans and development training and air operation's center training. This training provides core fundamentals to Airmen who coordinate air tasking orders and master attack plan requirements. Success in the past 12 years of air operations in Iraq and Afghanistan is the fruits of this training success.

Finally, equipment advancements enabled the successful execution of Warden's model. I am not arguing that success would not have been achieved without technological advances that occurred in stealth aircraft or precision munitions; it just would not have occurred as quickly and more ordnance would have been required.⁸⁴ The simple fact is, Desert Storm proved stealth-technology-enabled airpower operations to be more efficient than deploying the bomber and escort fighter packages of wars past, while technology increased munitions effectiveness. The result is more targets attacked with fewer sorties flown than ever before.

The United States' pursuit to maintain the latest-generation bomber and fighter aircraft and to seek continuous improvements in munitions technology and precision weaponry affirms the need for these capabilities in future wars. A result of this high-tech equipment pursuit is an inferred need of these assets to achieve decisive air superiority, interdiction, and close air support advocated by Warden.

Is the Air Force using Warden's systems targeting model to organize, train, and equip the force to meet defined targeting objectives today? I posit the answer is yes. If military strategists and leaders agree, then a question arises regarding the effective use of cyber power. Should a targeting model theory that enables system effects—either in a supporting, supported, or independent role—drive the Air Force cyber OT&E functions for cyber operations today? If so, can such a theory be developed from the concepts of the industrial web theory and Warden's targeting system previously discussed?

Summary

The word *intelligence* in the epigraph at the beginning of this chapter can have various meanings. Although Warden was referring to the intelligence needed about enemy disposition and capabilities necessary for effective targeting of centers of gravity, I argue intelligence can refer to the military genius Clausewitz advocates.⁸⁵

Military members must constantly study military history and pursue professional military and personal education to continuously develop effective military strategies, especially the targeting strategies I argue are key to military OT&E functions. Using learned skills and training through combat scenarios enables critical thinking about warfare with the ultimate objective of either preventing war with adversaries based on their fear of US capabilities or ending war quickly when it does occur.

The men who made up ACTS developed the art of aerial warfare and created foundational doctrine. Colonel Warden learned from doctrine and evaluated failures and successes to harness airpower's true potential in his five-ring targeting model. Although tables 2.3 and 3.5 appear similar, they are different in the foundational approach to applying airpower advocated by Warden. The strategic bombing targets promoted by ACTS directly supported the military functions and capabilities in some manner, whereas Warden's model targeted the national strategic targets that went beyond military centers of gravity. It was not just about attacking industrial and economic targets advocated by ACTS; a priority for the target sets was needed, something Warden clearly argues is critical while placing leadership at the center ring. Additionally, targets require simultaneous, unrestricted attack to achieve decisive strategic results. Escalation of warfare capabilities, like in Korea and Vietnam, reduces combined effects of weapon systems and limits results derived from attacking centers of gravity simultaneously when possible. Overwhelming the enemy can be decisive and lead to quick capitulation.

Warden's military and civilian education, combined with his operational experience and understanding of warfare, enabled him to postulate a decisive air campaign planning strategy. Although his theory was based on similar targeting principles espoused by early airpower advocates, Warden combined a priority schema with the overwhelming use of force to target objectives and create strategic effects. He was able to do this because he understood not only the capabilities of airpower, but its limitations and those imposed upon it by society.

Given the limited airpower theories both created and studied beyond ACTS and the 1930s, only Warden is considered to have made significant contributions to the thinking regarding the employment of airpower. The list of theorists from chapter 2 is expanded in table 3.5 to include Warden's theory.

TARGETING

Table 3.5. Airpower theorists and target objectives

Theorist(s)	Target Set(s)
Douhet	Population (cities)
Trenchard	War materiel, transportation, communications
Mitchell	Vital centers
de Seversky	All aspects of an industrial infrastructure
ACTS	Key economic nodes (war-making materials, transportation, electricity, oil)
Warden (updated)	Five rings (leadership, key processes, infrastructure, population, fielded military)

Created by author based on published documents.

It is now time to evaluate these same possibilities and limitations regarding the use of cyber power. We will begin the next chapter by evaluating potential constraints on targeting when using cyber power to achieve military and strategic objectives.

Notes

1. Sherry, *Rise of American Air Power*, 237.
2. Ibid., 361.
3. Crane, *American Airpower Strategy in Korea*, 6.
4. Ibid., 7.
5. Ibid., 186; and Anderson, "Air Warfare and Morality," 7.
6. Pape, *Bombing to Win*, 271.
7. Ibid., 92.
8. Ibid., 69.
9. Crane, *American Airpower Strategy in Korea*, 188; Steiner, *Bernard Brodie*, 46–64, 269 11n; and Brodie, "The Morale Factor in STRAP Planning."
10. Douhet, *Command of the Air*, 129.
11. Ibid., 10.
12. Zhang, *Red Wings over the Yalu*, 199.
13. Craig, *Destroying the Village*, 157.
14. Ibid.
15. Clodfelter, *Limits of Airpower*, 85.
16. Ibid.
17. Ibid.
18. Ibid.
19. Anderson, "Air Warfare and Morality," 7; Mommyer, *Airpower in Three Wars*; Futrell, *Ideas, Concepts, Doctrine*, 259; and Clodfelter, *Limits of Airpower*, 127.
20. Clodfelter, *Limits of Airpower*, 113.
21. Ibid., 140.
22. Randolph, *Powerful and Brutal Weapons*, 18.
23. Clodfelter, *Limits of Airpower*, 154.

24. Ibid., 157.
25. Ibid., 158.
26. Ibid.
27. Finney, *History of the Air Corps Tactical School*, 4.
28. Randolph, *Powerful and Brutal Weapons*, 130.
29. Pape, *Bombing to Win*, 175.
30. Watts, *Foundations of US Air Doctrine*, 45–46.
31. Cody, “AWPD-42 to Instant Thunder,” 36.
32. Olsen, *John Warden*, 22.
33. Ibid., 37.
34. Ibid., 22–37.
35. Ibid., 28.
36. Ibid., 32.
37. Warden, *Air Campaign*, 112.
38. Ibid., 113.
39. Ibid.
40. Hoig, Rosier, and Deer, *The Cheyenne*, 98.
41. Warden, *Air Campaign*, 34–35.
42. Olsen, *John Warden*, 66.
43. Clausewitz, *On War*, 619.
44. Warden, *Air Campaign*, 131.
45. Ibid., 52.
46. See the referenced essay in Olsen, *John Warden*, 108.
47. For a post-war refined discussion by Colonel Warden regarding his centers of gravity discussion and personally expanded details of each ring of his theory, see his work titled “Employing Air Power in the Twenty-First Century,” found in Pfaltzgraff and Shultz, *Future of Air Power*, 57–82.
48. For specifics on the strength of the Athens navy and alliances of both Athena and Sparta, see Strassler and Hanson, *Landmark Thucydides*, 14.
49. Ibid., 83.
50. Olsen, *John Warden*, 116.
51. Ibid., 114–15.
52. Clausewitz, *On War*, 117.
53. Ibid.
54. Col John A. Warden III, interview by the author, 30 January 2013.
55. Warden, *Air Campaign*, 150.
56. Thomas Kuhn defines an established paradigm as “an accepted model or pattern.” Although he was specifically discussing scientific revolution and the transition between one paradigm and another, something he calls a revolution, his understanding of a revolution is applicable to the transition from strategic bombing theorized by ACTS to Warden’s idea of targeting an enemy as a system. Prior to the Gulf War, airpower advocates argued for strategic bombing as the way to achieve victory with airpower. Warden’s model was a *revolution* in airpower thinking and was proven a success in the Gulf War. Warden’s theory then became the accepted model or pattern for employing airpower. Kuhn, *Structure of Scientific Revolutions*, 23.
57. Belote, “Warden and the Air Corps Tactical School.”
58. In efforts to delay a ground campaign, Warden briefed then–secretary of defense Dick Cheney about the cumulative effect of the operational air campaign. When the briefing was

TARGETING

completed, Cheney commented, “For the first time, I understand why you people are so confident about this whole thing.” Quoted in Olsen, *John Warden*, 231.

59. It is important to note that although Warden was a literary student of Clausewitz, he did not fully agree with all that Clausewitz espoused. Specifically, Warden believed Clausewitz’s attention on the “enemy’s will” had created challenges to strategic thinking within the military. Warden’s point is that the *will* of the enemy is not something military strategists can directly affect with military action. Enemy capabilities can be targeted, destroyed, or made ineffective in order to prevent the enemy from doing something friendly forces do not want to occur. Of the three broad objectives of disarming a country Clausewitz espouses, “armed forces, the country, and the enemy’s will,” it is the focus on the will Warden has concerns with. Warden, interview by the author.

60. Clausewitz states that even the ultimate outcome of war is not always to be regarded as final. The defeated state often considers the outcome merely as a transitory evil, for which a remedy may still be found in political conditions at a later date. It is also important to remember that according to Clausewitz, war is the means to reach political objectives. Since political objectives may change and are not always defined in such a way that prescribes success in war, there is no political recipe for guaranteed success in combat. Clausewitz, *On War*, 80–87.

61. Olsen, *John Warden*, 148.

62. Putney, “From Instant Thunder to Desert Storm,” 40.

63. Meilinger, “Ten Propositions Regarding Airpower,” 39.

64. Putney, “From Instant Thunder to Desert Storm,” 40.

65. Olsen, *John Warden*, 148.

66. *Ibid.*, 149.

67. The military objectives derived from these resources were withdrawal of Iraqi forces from Kuwait, restoration of Kuwaiti sovereignty, unimpeded flow of oil, and protection of American lives. Olsen, *John Warden*, 148.

68. *Ibid.*, 159.

69. Hallion, *Storm over Iraq*, 143.

70. Putney, “From Instant Thunder to Desert Storm,” 42.

71. *Ibid.*

72. During a discussion regarding the phase I offensive air campaign, a report by the Defense Technical Information Center highlights some of the challenges early intelligence communities had in providing information about Iraq and its actual capabilities and threats. See the Defense Technical Information Center review, 35. Additional information is found in Keaney, Cohen, and Gulf War Air Power Survey Review Committee, *Gulf War Air Power Survey*, 38.

73. Olsen, *John Warden*, 148.

74. *Ibid.*

75. Keaney, Cohen, and Gulf War Air Power Survey Review Committee, *Gulf War Air Power Survey*, 1.

76. *Ibid.*, 265–346, especially 305, for specific details on eight core strategic targets the airpower survey evaluated and the effectiveness of airpower against those targets.

77. Morrocco, “From Vietnam to Desert Storm.”

78. Keaney, Cohen, and Gulf War Air Power Survey Review Committee, *Gulf War Air Power Survey*, 12.

79. *Ibid.*, 39.

80. *Ibid.*, 40.

81. *Ibid.*, 161.

82. Ibid.

83. Hallion, *Storm over Iraq*, 209–19.

84. For a sample comparison of the number of targets each aircraft could engage and the number of munitions to strike each target, review the airpower survey results. As a sample, an F-111 (Vietnam-era aircraft still used in Desert Storm) required 14 Mk-82s to strike one radio station whereas an F-117 carrying two GBU-27s struck two separate targets on the same mission. Keaney, Cohen, and Gulf War Air Power Survey Review Committee, *Gulf War Air Power Survey*, 353.

85. Clausewitz's argument that the commander in chief be a statesman, but not cease to be a general, may not appear feasible to military leaders today. The point Clausewitz was making is that military leaders who are supreme commanders must understand the entire political situation in order to achieve the victory and the attainment of political objectives simultaneously. The difference in his writing and today is that at the time the military leaders were also potentially statesmen when not in war. Not all military members are intended to be military geniuses; otherwise the military would "be very weak." A military genius is one with the qualities of experience, observation, comprehension, and calm in war. Warden's advocacy for operational and strategic use of airpower and his conception of the enemy as a system which could be destroyed quickly by targeting key centers of gravity in order to achieve rapid political objectives show his understanding of the military as the means in achieving political ends. Clausewitz, *On War*, 100–12.

Chapter 4

Artifacts for Cyber Power Targeting

War is such a dangerous business that the mistakes which come from kindness are the very worst.

—Carl von Clausewitz
On War

The practice of warfare can thus be understood as the attempt to impose order over chaos, to exert control where it most threatens to elude, and to find predictability in the midst of uncertainty.

—Antoine Bousquet
The Scientific Way of Warfare

This chapter focuses on the considerations and challenges facing cyber warfare in relation to targeting adversary capabilities. For scoping reasons, and to avoid getting lost in vociferous discussions about the many varying concepts surrounding influences on cyber war or cyber warfare or the debate over definitions of cyber warfare, this chapter centers on three specific elements—*attribution, authorities, and centers of gravity*. Although these three affect the conduct of cyber warfare, this discussion does not intend to define what the US stance regarding each attribute should be, but rather posits discussion points for consideration by leadership and policy makers as cyber warfare concepts evolve and are employed in war.

As the US military strives to embrace a theory of cyber warfare, practitioners should not discard known principles of warfare in the other war-fighting domains—land, sea, air, and space—as current principles are just as applicable in the cyber domain. Given the lack of warfare experience in the cyber domain, academics and military advocates are left drawing logic parallels between other domains to justify ongoing efforts to organize, train, and equip forces within each military service. This action is a good start as parallels will aid development by drawing upon the many lessons learned from previous warfare, no matter in what domain the experience was gained. Gen Larry D. Welch, retired Air Force chief of staff, captures this point when he states that “the fundamental military objectives are essentially the same as in other domains.”¹ However, leadership should not inhibit new principles of warfare from developing as cyber operations evolve and experience is gained. Although the nature of war has not changed, its character continues to develop.

Cyber offers unique challenges which must be considered, war gamed, and standardized when possible. It also offers greater flexibility to the military commanders of tomorrow.

Principles of War for Airpower Revisited

AFDD 1 advocates unity of command, objective, offensive, mass, maneuver, economy of force, security, surprise, and simplicity, as well as unity of effort, restraint, perseverance, and legitimacy as the principles of war.² These principles are intended to “serve as valuable guides to evaluate potential courses of action” and are not a “checklist to guarantee victory.”³ It is relevant to show a correlation between service and joint doctrine since the Air Force is part of the joint fight.

JP 3-0 affirms every principle of war that AFDD 1 does, except “unity of effort.”⁴ The point in highlighting this disparity is that although US military forces operate toward and serve common political objectives, the services do not necessarily function with exactly the same principles of warfare. This does not change the individual services’ desired *ends* of achieving the political object, but it may change the *ways* and *means* it employs to get there. This example highlights the importance of not getting stuck on tradition or beliefs, but rather suggests that services are focused on the desired objectives while using available resources in proven and innovative ways. The challenge is—as it was with airpower when initially evaluated for military use—determining initial barriers to efficacy and working to resolve issues that prevent or delay cyber power’s use in warfare. This brings us to the crux of this chapter.

Challenges to Cyberspace

Kuhn stated that “electronic technologies and the electromagnetic spectrum” are what make cyberspace unique.⁵ I suggest that it is the estimated seven billion people in the world that make it unique.⁶ An increasingly wide range of social, political, economic, and military activities depend upon cyberspace, making it both a capability and vulnerability.⁷ With so much interest in what cyberspace can afford businesses, as well as individuals, and given its low entry cost, cyberspace has truly become a tool for *virtual expansionism*. The only limitation to cyberspace use is the innovation of people. For this reason, cyberspace has become a global commons.⁸

The notion of social or public good—common goods—dates back to Roman law. Roman law held that certain resources were unsuited for ownership by

individuals or governments; therefore they were distinguished as *res communis*, or a “thing (*res*) for everyone (*communis*),” and *res nullius*, or a “thing for no one.”⁹ *Res communis* was applied to air and sea domains, as they were perceived to be used by all. Today, space is considered a “global commons” and has support from advocates like the United States seeking to “assure the use of space for all responsible parties.”¹⁰ If cyberspace can be used by anyone with access without detracting from others, cyberspace is *res communis*. But is it really?

Actions within cyberspace in democratic societies have been primarily self-regulated up to now, although some simply view cyberspace as the “Wild West” of days past.¹¹ The belief that cyberspace is *res communis* stems from the erroneous notion that any one person using cyberspace cannot prohibit others from using cyberspace. I believe that is absolutely false. Although we could discuss a variety of ways that cyberspace can be limited by actors within the domain, a quick overview of a distributed denial of service (DDOS) attack makes the point. The intent of a DDOS attack is simply to temporarily or permanently disrupt the service between a host and the service provider. In other words, Internet communication is reduced by extremely slow processing or blocked completely.¹²

I conclude that humanity is prohibited from saving the commons through individual action by accepting “The Tragedy of the Commons” as outlined by Garret Hardin.¹³ Therefore, the only solution is to organize cyberspace based on bureaucratic law since self-regulation will not work.¹⁴ Gary Hart, a former member of the Senate Armed Services Committee, suggests that “establishing an international cyber security monitoring and management agency” may help stabilize this new global common.¹⁵ This move toward governance is not new, as “signs to govern cyberspace [have] slowly emerg[ed]” within the United Nations since 2004.¹⁶ That is not to say that the government should create or fully control the public good relevant as in a socialistic society. According to Mancur Olson, the challenge to government involvement is that “when the government provides collective goods it restricts economic freedom; when it produces the noncollective goods usually produced by private enterprise it need not restrict economic freedom.”¹⁷ For these reasons, government involvement should focus on “separate and selective incentives” to stimulate rational individuals to act in a group-oriented way.¹⁸ “Selective incentives can be either negative or positive,” but they must focus on the actors who challenge the social norms of a global common and cannot be indiscriminate in nature.¹⁹ Therefore, knowing who conducts cyberspace actions is critical, especially if negative incentives are required by those authorized to conduct such action in order to shape undesired cyberspace activities. This leads to a host of questions.

Why is attribution vital to cyberspace operations? Is attribution possible in cyberspace, or is it continually an Achilles Heel? Under what authority is cyber power wielded by military force, and are rules of engagement required for those operations? Is the use of cyber power limited to military forces? Does world globalization, as evidenced by the interconnectedness of business, economics, and societies to cyberspace, affect the wielding of cyber power? Does cyberspace further remove the warrior from morality concerns of warfare? These are not all the questions surrounding the use of cyber power, but they are some of the frontline ongoing points of discussion in academia, society, corporations, and the military.

As this chapter delves into the three elements of cyber power—attribution, authorities, and centers of gravity—it is important to begin from a baseline of what constitutes cyber war. Do *cyber war* and *cyber warfare* mean the same thing? Given the infancy of cyber warfare discussions, how to conduct cyber warfare and its potential limitations in war are good conversations to have. However, at some point, sound doctrine must be established and progressive efforts moved forward so the United States and the international community alike know the parameters of what actions within, through, or from cyberspace will constitute war with the United States. Otherwise, US citizens will continue to see comments from the US national security advisor such as, “[US businesses share serious concerns] about sophisticated, targeted theft of confidential business information, and proprietary technologies through cyber intrusion.”²⁰ US military forces see policy maker comments such as, “we will take action to protect our economy against cyber threats,” and wonder what type of military response is feasible.²¹ A cyber attack that does not cause visible kinetic effects reduces the response threshold versus an airplane flying into a building or an antisatellite rocket being fired. My question is, why is a cyber attack treated differently?

Knowing what constitutes cyber war, having a common understanding of it, and standardizing it across the US military services will enable efficient and effective OT&E functions. It also clarifies what rules or policies regarding cyberspace operations need to be created, modified, or removed both in the domestic and international environment. An additional benefit of common definitions is the purported standardization of tactics, techniques, and procedures regarding roles and responsibilities between military and nonmilitary cyber operating forces, which is muddying the operational world regarding domestic and international cyber power operations today. An operational pause occurs when determining who is authorized to respond to a threatening cyber event. This pause must go away if the United States wields cyber power the way John Boyd suggests is required to stay ahead of the enemy.²²

Cyber War Bytes

Thucydides reminds us that fear, honor, and interests are three strong motivators for war.²³ However, if an adversary's intentions are not known, then these motivators for war are no more than psychological operations. Although there are "psychological dimensions within any element of national power," cyber power should not be relegated to simply another means for conducting psychological operations.²⁴ However, cyber power can be one more capability to shape foreign perceptions of US military capabilities which are "fundamental to strategic deterrence."²⁵ The challenge is how to determine when cyber war occurs when a formal declaration of war is not declared, especially when pundits argue cyber war is ongoing every day.

Martin Libicki argues that technological and organizational innovations over the last few decades have created the potential for "nonobvious warfare."²⁶ Types of warfare that could plausibly be conducted in nonobvious manners include cyber warfare; space warfare; electronic warfare; drone warfare; sabotage, special operations, assassinations, and mining; proxy attacks; weapons of mass destruction; and intelligence support to combat operations.²⁷ Military professionals must understand that there is more to cyber warfare than the mundane adage of hackers attacking a system to disrupt its function, corrupt its data, or render the machine inoperable with a harmful execution file. Cyber power can influence not only warfare in cyberspace, but also capabilities in all war-fighting domains. However, cyber professionals must first understand what constitutes cyber war and cyber warfare before cyber war-fighting capabilities can influence actions across all domains.

Precursor to Cyber War, Cyber Warfare, and Attribution

For the US military, neither cyber war nor cyber warfare is clearly defined in open-source doctrine. The military should consider the principles of war suggested above when conducting cyber warfare; however, what we are talking about here is the basic definition of cyber war. With dramatists like Michael Gross saying "Stuxnet is the Hiroshima of cyber war" and attempting to draw similarities between cyber warfare and nuclear warfare, the antennas of those in the military defense business tend to go up.²⁸ Although this is an over-exaggerated analogy since Hiroshima killed an estimated 130,000 people, while Stuxnet is not known to have killed anyone, the warning of potential damage caused by cyber attacks like Stuxnet is valid.²⁹ When cyber capabilities are described as "a self-directed drone: the first known virus that, released

into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done,” those capabilities begin to sound like special military operations in action.³⁰ But does an attack like Stuxnet constitute cyber war? Does the destruction of another nation’s centrifuge-making ability, whether or not it is believed to be constructed for use in nuclear weapons, constitute war?³¹ That answer depends on one’s perspective on the attack. However, that discussion is left for future debate as it is outside the scope of this paper.

Cyber warfare is any act to contest or control the cyber domain in order to dominate opposing force capabilities in any or all war-fighting domains, while preventing an adversary the same freedom of action. Cyber warfare is the *ways* and *means* available to influence friendly and adversary capabilities in, through, or from cyberspace. Cyber war can be an independent form of limited war or, in conjunction with other forms of warfare, can escalate toward total war, but this distinction is irrelevant. Remembering that the intent of war is “to compel the enemy to do our will” is relevant.³² Cyber power, along with airpower and space power, are all *means* to influence an adversary’s will for the US Air Force.

What the Air Force cannot do is forgo the opportunity to think about and develop the *ways* and *means* of influencing war through cyber power, despite arguments like those of Thomas Rid. Aside from harshly criticizing Pres. Barack Obama’s national security policies, Rid believes the Obama administration is making “two crucial mistakes.”³³ By signing a November 2012 policy that includes offensive use of computer attacks, Rid claims the Obama administration “fail[s] to realize (or chooses to ignore) that offensive capabilities in cyber security don’t translate easily into defensive capabilities.”³⁴ Rid states that the administration “fail[s] to realize (or chooses to ignore) that it is far more urgent for the US to concentrate on developing the latter, rather than the former.”³⁵ This is exactly the trap of limited thinking that US military strategists cannot afford to fall into. It is not one or the other; these capabilities are not mutually exclusive. Adversaries do not think in limited terms of warfare and neither should US forces. I argue the defensive form of cyber war is critical, but not decisive. To be decisive in war, offensive capabilities are required and must be developed so they are available when called upon. Without US policy-making authorities to develop offensive cyber warfare capabilities, military forces are hindered by the political constraints Rid argues for.

Now we modify the Stuxnet scenario presented while applying the suggestion of Gross, and presume that the Stuxnet worm can “exploit” a target it specifically seeks out.³⁶ Since the worm affects the supervisory control and data acquisition (SCADA) of a system and the controls over a particular system

could be *owned* by someone else, the potential exists for catastrophic damage initiated by a cyber attack. Hypothetically speaking, the catastrophe that occurred at the Sayano-Shushenskaya hydroelectric plant in Khakassia, Russia, could have been caused by a SCADA attack.³⁷ Given today's virtual control of command systems via cyberspace, such as the one controlling the hydroelectric plant, the potential exists for an adversary to attack an unprotected system. It is conceivable that cyber attacks can have kinetic effects since 75 people lost their lives during the Khakassia incident and expensive resources were lost.

Knowing this capability exists, one has to ask the question, "could Stuxnet cause a nuclear weapon to destruct?" What about a nuclear weapon sitting on a launch pad waiting for the final "execution" command before being fired? It would not be hard to imagine this given the many known vulnerabilities within cyberspace in the open media these days. As shown by this oversimplified scenario of the potential threats within, through, and from cyberspace, it behooves military strategists to strive for clarity surrounding cyber power and its use in future warfare. One of the first and potentially most detrimental tasks in any decision regarding a response to a cyber attack is the ability to attribute who conducted an offensive action against the United States, its allies, or its interests.

Attribution Need Not Be 100 Percent in Cyberspace

Attribution is particularly difficult for a cyber attack.³⁸ I argue that with or without resolution of the attribution problem, warlike endeavors through cyber attacks are ongoing and will lead not only to cyber war but to war between great powers if steps are not taken now to corral these warlike activities. This opinion differs from an upcoming publication by Rid who argues that cyber attacks fall into three categories—sabotage, espionage, and subversion—but that cyber war has not happened and is unlikely to occur in the future.³⁹ However, since "economic and technological leads are likely to become more important in international politics" and some nations are on the verge of conflict over territorial control of various islands, it is likely that war could occur in the form of other cyber attacks like those ongoing today.⁴⁰ By acknowledging and allowing instead of condemning and preventing these warlike actions, "custom" is established every day throughout the international community which may affect future interests of US political objectives and national security.

If a nation-state declares war upon another nation based on a cyber attack, attribution for cyber attacks must improve. Libicki acknowledges the importance of "having a good idea of *why* a state carried out a cyber attack."⁴¹ But it

is also important to know *who* carried out the attack if no one claims responsibility. Col Matthew Hurley rightly acknowledges cyberspace attribution of intrusions and attacks as a problem for intelligence, surveillance, and reconnaissance professionals.⁴² In reality, this is a challenge for every American from the president down to every individual with Internet access, whether they know they have something to lose or not. If a cyber attack is intended to destroy, disrupt, degrade, or control an adversary's capability through the cyber domain or to steal corporate knowledge or the identity of an individual, the action must be attributable with a high degree of accuracy before law enforcement or an applicable instrument of power is called upon to respond.

Retaliation without attribution is like shooting a bullet into the dark without seeing a target. It wastes resources and potentially causes unintended damage or harm. What makes attribution so difficult in cyberspace is that the complexity of the Internet enhances an attacker's ability to hide the true source of an attack. However, do nations require a 100 percent attribution factor before responding to a crisis? Or can something like mutual assured destruction (MAD), albeit on a less critical scale than nuclear annihilation, theoretically work as international norms are developed regarding cyber attacks?⁴³ The authors of *Cyber Power and National Security* argue that attribution, or the lack of it, "does not holistically paralyze any attempt to think fruitfully about a cyber deterrence strategy."⁴⁴ Deterrence need not be as devastating as nuclear power to still be effective. A cyber deterrence concept may or may not focus on destroying people and property, as was the case with MAD. Cyber deterrence should lean more toward subtly negating a nation's military, industry, financial, or other socially dependent capabilities that are reliant upon cyberspace to function.

As improvements in new cyber forensic technology continue, experts like Dr. Kamal Jabbour acknowledge that "detecting attacks, attributing them to a source, estimating damage, and enabling response courses of action to contain the attack and limit the damage" are getting better each day.⁴⁵ Has the time come for US policy makers to claim that if a cyber attack is determined, within a defined percentage of tolerance, to have originated from a particular nation, an immediate response is justified? Will this type of policy aid in reducing the continually increasing number of cyber attacks?

Since there are varying degrees of active cyber attack responses—stopping an attack, diverting an attack to a honey pot, or conducting direct action against the machine conducting the attack—maybe it is time to start escalating real-time responses in an effort to reduce the overall number and intensity of attacks.⁴⁶ This response theory is analogous to public law enforcement of highway speed limits. When drivers on the road see posted speed limit signs,

those who want to avoid a fee or confrontation with law enforcement will obey the posted speed signs. Others may risk the confrontation based on the perceived reward gained by not obeying it. Simply put, each driver makes a cost/benefit comparison. If a nation publicizes a speed limit for all of its roads and on the same day announces that its police force will not enforce the laws due to other priorities, how effective do you think the speed limit signs will be? Sure, there will be those who follow the posting for reasons such as security, safety, or morality, but in reality, it does not matter. Without an enforcement mechanism, it is a waste of resources to post the signs in the first place.

"People are more willing to follow the direction of someone they view as an authority," Christopher Hadnagy and Phil Wilson said.⁴⁷ But who is the authority for the Internet? The Internet is touted for its openness and freedom of use, not to be constrained by laws or regulations governing its use. If that is the case, users of the World Wide Web may believe the threshold of response to an illegal action conducted online is minimal, even if a law is in place, just like an unenforced speed limit sign posted on the side of a highway.

Threats from cyber attacks may decline by changing the paradigm to enable an immediate response to illegal or harmful activity, followed by technological advancement to automate responses. Public attribution is also required once the counterattack is complete. In other words, the counterattack response must be openly claimed by those executing it.⁴⁸

The question then becomes, what type of response is warranted and how are unintended side effects prevented? Given the interconnectedness of operations throughout the Internet, if shutting down a computer server known to be conducting cyber attacks also shuts down the power controller for a nearby hospital, who has the authority to execute such an action? The right level of authority may be possible if it is known the server also controls the hospital power, but what happens when that information is unknown before a counterattack is conducted? Is the response justified?

This simple example highlights the constant challenge to cyber operations. It is understandable that attribution is desired before a response is initiated. However, if some risk is not accepted in cases where 100 percent attribution is not possible, then the current level of cyber attacks will continue to remain unchecked and grow as more societal functions migrate to Internet operations. For a nation like the United States who relies immeasurably on cyberspace for societal functions as well as military operations, this continual threat and loss of national treasure through ungoverned cyberspace is unacceptable. The "free-for-all encounters of one state duel[ing] with those of another" is indicative of the Greek Dark Age (1000–800 BCE), not a period the United States or the international community should strive to emulate.⁴⁹ Therefore,

the question to ask is should an offensive cyber force, or at least an active cyber defense force, conduct more operations in cyberspace today to counter rising threats? If the answer is yes, where should this force reside and under what authorities will it operate? Where the force should reside is beyond this treatise, although chapter 5 alludes to a recommendation.

Governing Authorities

In a statement almost two years ago, Homeland Security secretary Janet Napolitano acknowledged that “a comprehensive international framework” to govern cyber behaviors is at “a nascent stage.”⁵⁰ Research shows that defined and accepted authorities, either for domestic governance or international laws governing cyber security, are sparse at best. However, this does not mean that a “comprehensive cyber security treaty is a pipe dream,” as some experts suggest.⁵¹ What it does suggest is that rules to govern cyberspace may best be tackled one small bite at a time, instead of pursuing an overarching international policy from the outset. If cyberspace is a global commons, then applying governance to operations within cyberspace after societies have been using it for more than two decades will be a challenge, but not impossible. Cyberspace will be, as James Forsyth suggests, “what great powers make it.”⁵² This will be the case even as lesser powers, nongovernmental agencies, and criminals attempt to have their voices heard through actions deemed unacceptable between nation-states.

If we accept the premise that “the current state of cyberspace and its users does not meet most conditions that encourage self-organization” and that tragedy of the cyberspace commons is inevitable in its current state, then government controls are necessary.⁵³ Without controls, the nonviolent actions in cyberspace today—sabotage, espionage, and subversion—will continue to escalate. When the time comes that great powers are no longer willing to tolerate the nonviolent cyberspace actions, the propensity for violence not only exists, it perpetuates each day cyberspace is allowed to operate ungoverned. This is especially true if one accepts the work of Kenneth Waltz.⁵⁴ Waltz states that “the evilness of men, or their improper behavior, leads to war.”⁵⁵ Therefore, it is time to stop accepting violations as the norm in cyberspace and set and enforce acceptable standards while encouraging international institutions to emulate them. To do this, the United States must develop domestic sovereignty regarding cyberspace.

“Domestic sovereignty refers to the ways in which internal affairs are conducted: specifically, how authority is organized within the state and how ef-

fective is the level of control these political structures exert,” Betts and Stevens said.⁵⁶ A challenge to implementing the required level of controls is presumably caused by the lack of understanding threats from cyberspace by the average user of the domain. Timothy Sample said that “we haven’t yet experienced the destruction of a national-level cyber attack . . . and the assumption is there is more time.”⁵⁷ From my perspective, time is rapidly running out.

“Attempts to control citizens’ activities through the exercise of various forms of power in cyberspace have met unsurprisingly with resistance,” Betts and Stevens continued.⁵⁸ Just last year, cyber legislation that would have offered “protection for companies willing to work with the government to help detect and stop cyber attacks,” failed to pass the Senate.⁵⁹ How can the DOD protect the security and ensure effective operations of US critical infrastructure—including energy, banking and finance, transportation, communications, and the Defense Industrial Base—which rely on cyberspace?⁶⁰

One method for establishing cyberspace governance, for those areas in which national security concerns outweigh all others, “is a highly regulated online environment in which national cyberspace maps onto national physical borders and mirror national norms and standards.”⁶¹ This attempt would allow each nation the freedom to establish rules and governance enforceable by internal regulations. This option does not forgo the need for international standards regarding acceptable behaviors in cyberspace. It only acknowledges the need to address domestic authorities first and then recommends leadership by example just as the United States has done many times before.

One main reason to argue for domestic policy and enforcement before international endeavors can be solidified is that cyber security is not the same as past US challenges. “The arms control regime and the World Trade Organization (WTO) are illustrative” to a potential international cyber regime, James Forsyth said.⁶² The difference between these two and a regime to manage cyberspace is the level of access and influence. Arms control was centered on nuclear deterrence. How many individuals had, or have today, access to nuclear weapons or the related technology? The WTO and its predecessor, the General Agreement on Tariffs and Trade, “led the world toward a more service-oriented economy.”⁶³ Again, a question is how many individuals actually conduct global trade or worry about fair globalization efforts throughout society? Any change to cyberspace control mechanisms theoretically impacts every individual with domain access. For this reason, there are many more voices to listen to when trying to establish a regime intended to minimize cyber security threats. This is also why examples of past regimes, like arms control or the WTO, may be a good starting point for regime discussions but should not prescribe the initial solution. Because cyberspace is such a dynamic environment,

it may be wise to pursue domestic authorities first, and then expand to international standards based on experience and leadership gained from the initiative.

For the United States to pursue a path of domestic cyberspace governance, the rhetoric that USCYBERCOM is the defender of critical national cyberspace infrastructure has to stop. Otherwise policy makers must give USCYBERCOM full lines of responsibility with applicable authority to mandate security practices, standards, and enforcement mechanisms to ensure compliance. This does not currently exist within USCYBERCOM. With about “90% of the relevant infrastructure owned by the private sector,” DOD does not control the majority of US cyberspace.⁶⁴ “Cyber threats to US national security go well beyond military targets and affect all aspects of society,” the DOD strategy reports.⁶⁵ Until this authority and responsibility bridge between military and commercial industries is closed, cyber vulnerabilities for critical national infrastructure will continue to exist. By looking within the federal government to see that these gaps exist, one can imagine the void between government and commercial entities.⁶⁶ By defining domestic policy in legislation—which directs that the national security interests of cyberspace be placed under the full responsibility of one agency—publicizing it, and then enabling authorities to enforce the policy, cyber threats can be mitigated and overall cyber security increased.

Enforcing cyberspace policy is not the same as enforcing rules in the other four domains—land, air, sea, and space. For example, when an unauthorized ship enters a sovereign nation’s waters, it is detected, the responsible agency takes action, and attribution is quickly determined. The same actions can occur in air and space. The same is not necessarily true for cyberspace, at least not today. In America, if a military cyber force were to offer help to a nongovernmental agency, this would violate the Posse Comitatus Act of 1879, unless first authorized by Congress. Current regulation “restricts the use of military forces in civilian law enforcement within the United States, unless it is within a federal government facility.”⁶⁷ Given these challenges, a first place to start enforcing cyber security is by evaluating roles and responsibilities of those tasked with protecting cyberspace.

Table 4.1 highlights some of the disparate roles that seemingly share lines of operations. If, after reviewing the different title responsibilities and the agencies tasked with executing the assigned roles, the reader walks away with a clear understanding of who is executing what and under what authority while perceiving a clear break in the lines of responsibility, then he or she is doing better than many professionals operating in the cyber realm. For example, if cyber attacks are occurring and US corporate secrets are being stolen, who is responsible for recognizing and reporting the attack, taking immediate

action to stop the attack if it is in progress, or recovering the data and shutting down the attacker's capability to prevent further attacks?⁶⁸ Are all of these options viable, and should they all be executed once an attack is identified?

Responses to the questions above will be as varied as the number of individuals who answer. In reality, they should not be. If someone walked into your home and stole a personal piece of property, legal rules govern that action, along with responsible agents to act on behalf of the offended. The same goes for corporations. If one company steals a patent-protected idea from another company, rules are in place to file a claim and potentially recover the losses. Those who conducted the illegal act are then held responsible for restitution and costs associated with legal action. Can cyber security laws be done the same way? If so, they undoubtedly must occur at a much quicker rate than the examples given.

Table 4.1. US cyber authorities and current title responsibilities

Title	Key Focus	Principle	Role in Cyberspace
Title 6	Homeland security	Department of Homeland Security	Security of US cyberspace
Title 10	National defense	Department of Defense	Organize, train, and equip US military forces for offensive & defensive cyber operations (OCO & DCO)
Title 18	Law enforcement	Department of Justice	Crime prevention, capture, and prosecution of criminals operating in cyberspace
Title 32	US national defense and civil support	State Army and Air National Guard	Domestic consequence management
Title 40	Chief information officer	All federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies
Title 50	Military, foreign intelligence, and counterintelligence activities	Commands, services, and agencies under DOD and agencies under ODNI [Office of the Director of National Intelligence]	The essential authority for computer network exploitation (CNE)

Reprinted from "US Code-Based Authorities Relevant to Cyber Operations," bullet background paper (Washington, DC: Headquarters, US Air Force, 2012).

For cyber security to work, overlaying the existing principles for national defense in the other four domains may not be the solution. The speed at which cyber attacks occur, change, reoccur, or stop is what makes cyber security so different from any other warfare domain. The time available to conduct inter-

agency coordination between domestic and international cyber forces—Title 32, National Guard, and Title 18, Law Enforcement, versus Title 10, National Defense—will not exist during an initial cyber attack. An agency with full responsibilities for cyber security may be required to detect and mitigate these threats. A cyber force within such an agency would eliminate confusion about lines of responsibility and consolidate all military, civilian, and corporate entities under one authority for policy standardization and efficient execution. It is important to remember, especially in democratic societies like the United States, that this attempt to standardize cyber security policy and enforcement focuses on national security interests. This effort could expand to private industry based on each business's choice to opt in or opt out of the stringent requirements set by this new organization. This is not the recommendation here. It would not be mandated for any industry not deemed critical to national security.

No matter what course of action the United States chooses for increased cyber security, any path toward defining acceptable standards, publishing domestic and international policy, and empowering an overarching cyber force responsible for US cyber security of national security interests is a move in the right direction. The United States cannot continue down the path of having “no overarching framework legislation in place” for cyber security.⁶⁹ The current path is costing the United States an unquantifiable amount of technological and economic loss.⁷⁰

Centers of Gravity and Cyberspace

Lt Gen Larry James, deputy chief of staff for intelligence, surveillance, and reconnaissance, recently sponsored a study to “determine how the Air Force can better integrate cyber and space target intelligence analysis and materials to create cross-domain target intelligence.”⁷¹ Although the findings of this study are not projected for completion until October 2013, it undoubtedly supports the 2012 Air Force Targeting Roadmap initiative. Managed by the Air Combat Command, the road map is intended to “provide fundamental guidance on how to better organize, train, equip, conduct, and manage [Air Force] targeting-related personnel and resources to ensure efficient and effective targeting operations during peacetime, contingency, and war.”⁷² Inherent in two of the five focus areas within the road map is the concept of centers of gravity. Understanding centers of gravity will not only drive a focused intelligence gathering campaign, it will drive strategic thinking and planning before and during engagements with an adversary. For these reasons, it is critical

not only for the Air Force intelligence community to understand centers of gravity, but for all cyber forces who plan and execute all of the OT&E functions and their leaders to understand them as well. Additionally, understanding these concepts allows for the introspection of friendly vulnerabilities as seen by the adversary.

Published US military doctrine is important for today's warriors to understand potential centers of gravity, but so is having an understanding of doctrine and military thinking around the world. A 2007 publication by the Military Science Publishing House in Beijing claims information warfare aims at "seizing control of information" and "is a new form of war."⁷³ The publication claims that "whoever gains information supremacy in war will hold in his hands the initiative of war," and "information capability has become the most important indicator to evaluate combat capability."⁷⁴ Beliefs such as these, combined with tautology such as "the Kosovo War was the first war to involve cyberspace confrontation and that every war since would involve cyberspace confrontation," present the growing importance of cyberspace.⁷⁵ Despite the fact that a true cyber war—in the sense of two air forces or two ground forces battling it out until political objectives are achieved—has not occurred, nations continue to enhance cyber warfare capabilities. To improve cyber warfare readiness, US forces must understand centers of gravity concepts to either achieve or aid in the achievement of combatant commander requirements. This is especially true when governments around the world consistently identify "US logistics and C4ISR systems as the most important centers of gravity to target in a conflict" in the future.⁷⁶

It is important to define the concept of centers of gravity. First, Clausewitz called centers of gravity "the hub of all power and movement, on which everything depends."⁷⁷ Second, JP 5-0 defines centers of gravity as "a source of power that provides moral or physical strength, freedom of action, or will to act."⁷⁸ Finally, Marine Corps doctrinal publication (MCDP) 1 states that "centers of gravity are any important sources of strength."⁷⁹ To help determine centers of gravity, MCDP 1 asks three questions: (1) which factors are critical to the enemy?, (2) which can the enemy not do without?, and (3) which, if eliminated, will bend him most quickly to our will?⁸⁰ From each of these definitions, the common attribute determines where the center of power comes from. Whether this power provides moral or physical strength, or enables freedom of movement or action, are all derivatives of the enabling power.

The human body provides an incredible example for illustrating centers of gravity analysis. The human body would not function without a heart, but today's technology can keep a human body alive with an alternative power source. Regardless of this argument, the center of gravity is still the same,

although in a different form. The point is that the brain, a source of power, can provide the will for action while the physical body provides the capability. The hands and feet provide physical strength and movement but are attributes of “the system” and not the center of gravity of the human body. Without blood flow and oxygen, the brain would cease to function and eventually the control center for the body—a system—would cease to operate together coherently. This analogy may lead to questions for the strategist who seeks a true understanding of centers of gravity. One question is how does one differentiate between true centers of gravity and attributes of the system surrounding a center of gravity? To employ resources efficiently and not waste them, it is critical to focus on true centers of gravity. Another question may be, if there is more than one center of gravity in war, can it change? Dr. Joe Strange of the US Marine Corps War College and Col Richard Iron of the UK army help answer these questions.

Aside from interpreting Clausewitz’s theories on centers of gravity and highlighting misinterpretations between his true meaning and the perceived meaning by practitioners of warfare, Strange and Iron draw two distinct characteristics relevant to understanding centers of gravity. The first is that the “physical centers of gravity [which] function as active agents” which they say “endeavor to destroy the enemy’s capability and will to resist.”⁸¹ In other words, this physical center of gravity may be like a physical capability—an army, navy, or air force. The second characteristic is “moral centers of gravity [which] function as active agents that influence or control physical centers of gravity.”⁸² Drawing upon Clausewitz’s examples, Strange and Iron highlight “the capital” in countries of domestic strife, or “community interests” among alliances, and finally “personalities of the leaders and public opinion” in popular uprisings, as specific moral centers of gravity. In other words, moral characteristics are not easily measured or identified, let alone easily targeted, during warfare. Thus we begin to see the challenges to identifying centers of gravity. If destroying centers of gravity is integral to the rapid conclusion of war, accurately identifying them is an absolute must.

Physical centers of gravity appear definable through effective intelligence resources and analysis of the enemy as a system. If a nation relies heavily upon a military force as its mechanism to mitigate or deter threats, then most likely that force is a center of gravity for that nation. That same force may be a moral center of gravity to the society and political body relying on the force for protection. If defeat were to befall the force, the will of the nation may fall with it, but that is not a guarantee.⁸³ To help bring clarity in identifying centers of gravity, we lean once again on Strange and Iron.

Strange and Iron in their second publication on centers of gravity analysis describe a useful model with four interrelated concepts.

1. Centers of gravity are physical or moral entities that are the primary components of physical or moral strength, power, and resistance.
2. Critical capabilities are capabilities that can destroy something, seize an objective, or prevent you from achieving a mission.
3. Critical requirements are conditions, resources, and means that are essential for a center of gravity to achieve its critical capability.
4. Critical vulnerabilities are those critical requirements that are deficient, or vulnerable to neutralization or defeat that will contribute to a center of gravity failing to achieve its critical capability.⁸⁴

By examining this model, one concludes that critical capabilities and requirements are inherent to critical vulnerabilities. Those critical vulnerabilities are essential targeting objectives to defeat an adversary's center of gravity. With training, strategists and planners can apply this model "to any conflict" to determine target objectives.⁸⁵ As is often the case, historical analysis determines true centers of gravity after hostilities; however, this same historical analysis helps shape better decisions in choosing centers of gravity to target in the future. The challenge is figuring out how to use all available intelligence resources to understand the adversary and analyze past experiences to identify what an adversary's physical and moral centers of gravity are before hostilities begin and then remaining vigilant to any changes once war fighting begins.

Strange and Iron conclude their model with an overview of centers of gravity and critical vulnerabilities in the 1991 Gulf War Campaign against Iraq. Although the view presented by Strange and Iron appears to be ground centric, their example works well with the chapter 3 overview of a contemporary air-power theorist, retired colonel John Warden. The associations are similar in that both models are defined by objectives and focus on centers of gravity. Using Strange and Iron's model, the overall campaign had the centers of gravity and critical vulnerabilities (table 4.2).⁸⁶

Table 4.2. 1991 Gulf War: centers of gravity and critical vulnerabilities

	Strategic	Operational	Tactical	Physical	Moral	COG	CV
Saddam Hussein	X				X	X	*Command and control
Iraqi IADS		X		X		X	US high-tech, electronic, and stealth capabilities
Republican Guard		X		X		X	Dependence on friendly reconnaissance assets and unable to see through smoke and haze
Iraqi artillery units			X	X		X	Dependence on IADS and Republican Guard to keep US-coalition forces at bay

*Command and control was not listed as a critical vulnerability by Strange and Iron. I added it based on my understanding of the first ring in Warden's model.

Derived from Dr. Joe Strange and Col Richard Iron, "Understanding Centers of Gravity and Critical Vulnerabilities," Part 1, 7–16, <http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf>.

During the course of analysis development both enemy and friendly centers of gravity should, when possible, be analyzed and considered before engaging in conflict. Also, propositions regarding improvements in defining centers of gravity or their attributes should not be overlooked. Just as the character of war continues to evolve, so too does the war fighter's understanding. The suggested theory that "future critical factors" influence "critical factor analysis" in later phases of warfare may be one such example.⁸⁷ By staying abreast of doctrinal changes, strategic think-tank discussions, and academic research, military commanders will be well suited for tomorrow's war—should it come.

Given that many war-fighting capabilities—command and control; global positioning; information, surveillance, and reconnaissance; precision munitions; and much more—rely directly or indirectly upon cyberspace and the fact that military organizations around the world believe that information warfare "is a new form of war," the criticality of conducting full spectrum operations in, through, and from cyberspace is evident in the future success in war.⁸⁸ By maintaining an understanding of the centers of gravity presented by Strange and Iron and applying the concepts of an enemy as a system pre-

sented by Warden in chapter 3, cyber warfare practitioners have many lessons to draw upon for success. However, this art of war is not for cyber warriors alone, but for commanders in all domains of warfare to understand and incorporate across weapon system platforms and war-fighting domains. This will aid not only in the development of the Air Force cyber-power targeting theory presented in chapter 5, but cyber power doctrine for US military forces and policy makers alike.

Additional Artifacts for Further Evaluation

A plethora of artifacts exist beyond the attribution, authority, and centers of gravity discussed that affect cyber power and those who choose to wield it for war. Three additional areas I consider for in-depth analysis include escalation, proportionality of cyber warfare, and the morality of cyber war. Specifically, have these areas changed the nature of war as some argue? Or is cyber war the continued advancement in warfare given new technologies resulting in a character change of war?

From cavalry and gunpowder to mechanized infantry and airpower, each change in technology led to changes in how warfare is conducted. The stirrup is said to be the “third [evolutionary] period” of the use of the horse in battle.⁸⁹ The stirrup “replaced human energy with animal power, and immensely increased the warrior’s ability to damage his enemy. It made possible mounted shock combat.”⁹⁰ Gunpowder led to rifles which replaced the long bow and crossbow. Once rifles were used, experience and continued advancements in technology allowed for increased rifling techniques and better accuracy, along with advancements in the weapons themselves. Ultimately the mass production of rifles allowed the infantry to increase the volume of fire, thus creating an advantage for those who used it. Next, mechanized infantry sought to replace mounted cavalry and speed the rate of warfare. Finally, the advent of airpower enabled adversaries to occupy the vertical flank of the day. For nations who can afford the technology and employ airpower effectively, airpower enables true control of the battlefield. However, airpower did not eliminate the need for ground forces to hold the battlefield once the enemy had withdrawn or been defeated.

This short historical review highlights critical technological milestones that directly affected the conduct of warfare. In other words, these changes in technology drove innovative means, employment methods, and doctrinal changes, but none of them led to a change in the nature of war. David Lonsdale captures this point when he claims that “the nature of war is the same as it was

in all past and all future ages!”⁹¹ Despite Lonsdale’s proclamation, some confusion regarding whether or not the nature of war changes may come from Clausewitz’s claim that “war is a chameleon because it changes nature in some degree.”⁹² However, it is important to understand the rest of Clausewitz’s writing before claiming that he believed the nature of war changes. He said that “war as a whole [is] in relation to the predominant tendencies which are a trinity: primordial violence; probabilities and chance; and subordination of a political instrument.”⁹³ In simpler terms, the Clausewitz trinity is best understood as “the people; the general and his army; and the Government.”⁹⁴ With this understanding, it may be more accurate to restate that when Clausewitz said “war is a chameleon because it changes nature in some degree,” he was referring to the character of warfare and used the word “nature” in the sense that with new technology, an evolution in the conduct of war would occur. Without further digression, the intent here is to highlight what can be learned from past changes in warfare while accepting that the nature of war has not and will not change and recognizing that the character of war has and will continue to change with each new technology.

Specifically, how have the previous warfare technology alterations changed the potential for escalation and proportionality of warfare and morality in war? Are there patterns to these changes that can shape cyber warfare doctrine and tactics, techniques, and procedures for tomorrow’s military? How do military forces employing cyber power measure the risk of unintended consequences when launching a cyber weapon? Can those forces minimize collateral damage to a target in or through cyberspace like precision-guided munitions or a special operations team? How do tomorrow’s warriors not become catatonic to the loss of life so far removed from the battlegrounds where blood is spilled? These are difficult questions. If cyber power can cause catastrophic kinetic damage as some believe, how primordial is the violence when the enemy has no face but is rather an “enter” key away from destruction? Maybe cyber warfare truly enables countries to fight what Roger Trinquier calls “modern war; war that allows the military to kill more and more of the enemy at greater and greater distances, thus reducing the cruel and brutal physical contact with the enemy.”⁹⁵

Summary

Attribution, authorities, and centers of gravity are but a few of the critical aspects to wielding cyber power effectively. Although 100 percent certainty regarding attribution is desired, it may not always be attainable. If the United

States is going to curb the growing trend of cyber attacks against areas of interest regarding its national security, a change in strategy is required. This change is obviously not a one-shoe-fits-all strategy; there will be trial and error as it will not be right the first time. By publicizing US intentions regarding offensive and active-defense cyber operations, the United States will begin to put enforcement mechanisms behind the rhetoric of previous years in regard to cyber security. When adversaries can expect a response to threats they initiated, the cost of any cyber attack goes up theoretically.⁹⁶ Now the adversary must determine the benefit gained from his or her action, potentially more so than in the past.

The level of response and authority to conduct such a response may change with each cyber event. The United States must remove the paradigm chains caused by operating in various war-fighting domains. Some laws and rules of engagement may be spread across the spectrum of conflict, but others may not easily support cyberspace operations. Those gaps must be exploited before war begins and cyber operations are employed. If not, delays to operations will surely occur, which will put the United States behind in the OODA loop decision cycle, thus potentially losing valuable time and effects against the adversary.

Finally, understanding centers of gravity, both those of the United States and of potential adversaries, will shape the battlefield. It can also drive prewar efforts to OT&E forces so when warfare begins, forces are not just beginning to understand how to use cyber power effectively to influence, disrupt, degrade, destroy, or control an adversary's capabilities through cyberspace operations. Developing critical capability, critical requirement, and critical vulnerability descriptions can help shape early operations and identification of true centers of gravity. Without them, delays to all five war-fighting domains may occur.

These three artifacts of cyber operations are but a small piece of the chaotic environment known as cyberspace.⁹⁷ The proverbial tip of the iceberg is what these three areas represent. What concerns war fighters, and potentially policy makers who guide war-fighting actions, is the 80 percent of the iceberg that remains below the surface—we have not begun to think about it critically or truly understand the complexities it brings to this technologically globalized world in which we live. However, for the Air Force, that is exactly what the remainder of this thesis attempts to address. What should the US Air Force target with cyber power? Can Air Force cyber power have strategic impact? Does an Air Force cyber-power targeting theory help the service to organize, train, and equip cyber forces for tomorrow's wars?

Notes

1. Welch, "Cyberspace—The Fifth Operational Domain."
2. AFDD 1, *Air Force Basic Doctrine*, 30.
3. Ibid.
4. JP 3-0, *Joint Operations*, I-2.
5. Daniel Kuehl, "From Cyberspace to Cyber Power," in Reveron, *Cyberspace and National Security*, 34.
6. Worldometers, "Current World Population."
7. Kuehl, "From Cyberspace to Cyber Power," 34.
8. The term *global commons* relates to the freedom to use the electromagnetic spectrum in order to conduct cyberspace activities. Although manmade technology that enables cyberspace operations may be controlled by geographical boundaries and nation-state rules, it is the electromagnetic spectrum that is *res communis*. A challenge from an international perspective is defining what part of cyberspace (the collective electromagnetic spectrum and technology to use cyberspace) is *res communis*. Given the reliance of other domains upon cyberspace, it can be argued that other domains depend on cyberspace for increased effectiveness: "Therefore, temporary disruptions of one global common can undermine the efficiency of the others." Valeri, "Countering Threats in Space and Cyberspace," 2.
9. Dolman, *Astropolitik*, 97.
10. Avis Lang claims most of the world's scientists recognize that space is a global common in the "Editor's Note" of Tyson and Lang, *Space Chronicles*, xiv; and *National Space Policy of the United States of America*, 3.
11. Gregory Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer, Starr, and Wentz, *Cyberpower and National Security*, 274.
12. Distributed denial of service attacks are an attempt to saturate a network by overwhelming its network capacity and thus limiting inbound and outbound traffic via the network. For concerns regarding DDOS filtering and an adversary's counteractions, see Amoroso, *Cyber Attacks*, 60–61.
13. Garret Hardin was an American ecologist who warned of the dangers of overpopulation. For an overview of the "Tragedy of the Commons," see Dolman, *Astropolitik*, 97–103.
14. Ibid., 103.
15. Hart, "After bin Laden," 19–25.
16. Maurer, *Cyber Norm Emergence at the United Nations*.
17. Olson, *Logic of Collective Action*, 95.
18. Ibid., 51.
19. Ibid.
20. Bill Gertz, "DC to Beijing: Stand Down on Cyber," *Washington Free Beacon*, 11 March 2013, <http://freebeacon.com/d-c-to-beijing-stand-down-on-cyber/>.
21. Ibid.
22. Without the ability to get inside the OODA loop of an adversary, military commanders will find it impossible to comprehend, shape, adapt to, and in turn be shaped by an unfolding evolving reality that is uncertain, everchanging, and unpredictable. Boyd, "Essence of Winning and Losing."
23. Strassler and Hanson, *Landmark Thucydides*, 43.
24. Goldstein and Findley, *Psychological Operations*, 8.
25. Ibid.
26. Libicki, "Specter of Non-Obvious Warfare," 88.
27. Ibid.

28. Gross, "A Declaration of Cyber-War."
29. Michael Sherry provides a reference derived from the Committee for Compilation, *Hiroshima and Nagasaki*, trans. Eisei Ishikawa and David L. Swain (New York: Basic Books, 1981), 420–21, which estimated 130,000 lives were lost in Japan by the atomic bomb in Hiroshima. Sherry, *Rise of American Air Power*, 406.
30. Gross, "A Declaration of Cyber-War," 2.
31. The Tallinn Manual would lead one to believe the answer is "yes." If this is the case, are nations setting a precedent by not classifying these actions as acts of aggression or acts of war accordingly? For more specifics, see Schmitt, *Tallinn Manual*.
32. Clausewitz, *On War*, 75.
33. Rid, "Cyber Fail."
34. Ibid.
35. Ibid.
36. Exploitation enables the use of a discovered vulnerability to be used for the purpose an adversary might have. Amoroso, *Cyber Attacks*, 35.
37. To read more about the Say-Shushenskaya hydroelectric plant incident and see pictures of visual destruction, see Boyko, Popov, and Krajisnik, "Investigating the Sayano-Shushenskaya Hydro Power Plant Disaster."
38. Libicki, "Specter of Non-Obvious Warfare."
39. Information from the abstract of Rid, "Cyber War Will Not Take Place," is found at <http://www.amazon.com/Cyber-War-Will-Take-Place/dp/0199330638>.
40. Kenneth Waltz discusses reasons countries gain during their development by adopting technology from other countries with more advanced economics. Waltz, *Theory of International Politics*, 179.
41. Libicki, *Cyberdeterrence and Cyberwar*, 75.
42. Hurley, "For and From Cyberspace," 12–32.
43. Mutual assured destruction was originally developed by John von Neumann. Bernard Brodie applied it to the "strategy for a missile age" as found in Brodie, *Strategy in the Missile Age*. The MAD theory addressed the issue that short of preventive war, there was no alternative to doing whatever was necessary to erase the perceived advantage of a first strike. The end result of this theory was that once a missile launch was detected and two of three criteria for confirming the launch location was determined accurate, then an immediate response would be initiated. For details on MAD, see McDougall, *Heavens and the Earth*, 212.
44. Kramer, Starr, and Wentz, *Cyberpower and National Security*, 309.
45. Jabbour, "Science and Technology of Cyber Operations," 15.
46. A honeypot is a computer, usually virtual, without any security safeguards—in other words, designed to be infected by malware or to subvert an attacker's efforts. Bowden, *Worm*, 248.
47. Hadnagy and Wilson, *Social Engineering*, 199.
48. An understanding of deterrence theory, as espoused by Thomas Schelling, is relevant here. Deterrence is concerned with influencing the choices that another party will make and doing it by influencing the expectations of how we will behave. For more on deterrence theory, see Schelling, *Arms and Influence*.
49. Ferrill, *Origins of War*, 91–94.
50. Napolitano, "Remarks by Secretary Napolitano."
51. Segal, Greenberg, and Waxman, "Why a Cybersecurity Treaty Is a Pipe Dream."
52. Forsyth, "What Great Powers Make It."
53. Hurwitz, "Depleted Trust in the Cyber Commons."

ARTIFACTS FOR CYBER POWER TARGETING

54. Kenneth Waltz was a political scientist at the University of Berkley and Columbia University. He was one of the most prominent scholars in the field of international relations. Walt, "Kenneth N. Waltz."

55. Waltz, *Man, the State, and War*, 39.

56. Betz and Stevens, *Cyberspace and the State*, 64.

57. Sample, "Calling for a National-Level Doctrine."

58. Betz and Stevens, *Cyberspace and the State*, 68.

59. Cheryl Pellerin, "DOD Officials Cite Advances in Cyber Operations, Security," *American Forces Press Service*, 14 March 2013, <http://www.defense.gov/news/newsarticle.aspx?id=119532>.

60. DOD, *DOD Strategy for Operating in Cyberspace*, 1.

61. Betz and Stevens, *Cyberspace and the State*, 71.

62. Forsyth, "What Great Powers Make It," 105.

63. Ibid.

64. Betz and Stevens, *Cyberspace and the State*, 71.

65. DOD, *DOD Strategy for Operating in Cyberspace*, 4.

66. See the US Department of Energy's (DOE) inspector general findings regarding dozens of unaddressed cyber vulnerabilities at key DOE facilities, "including ones dealing with nuclear programs." Although cyber vulnerabilities within the DOE have declined from 56 to 38 since 2011, 22 of the open 38 are brand new vulnerabilities, while 16 remain unresolved from previous inspections. This level of vulnerability seems unacceptable to critical national infrastructure; however, without a concern for accountability, who is managing the oversight for responsibility? For further details, see Marcus Weisgerber, "Report: DOD Could Save Billions with New Military Strategy," *DefenseNews*, 15 November 2012, <http://www.defensenews.com/article/20121115/DEFREG02/311150001/Report-DoD-Could-Save-Billions-New-Military-Strategy>.

67. Fischer, "Federal Law Relating to Cybersecurity," 20.

68. See recent concerns between the United States and China regarding the loss of US corporate secrets due to cyber attacks. William Wan, "US Presses China on Cyber Attacks," *Washington Post*, 20 March 2013, http://www.washingtonpost.com/world/asia_pacific/us-presses-china-on-cyberattacks/2013/03/20/ef11a3d0-916a-11e2-9173-7f87cda73b49_story.html.

69. Fischer, "Federal Law Relating to Cybersecurity."

70. To see estimates of what some US companies, as well as other nations, are spending to counter cyber threats or repair losses caused by cyber attacks, see Ponemon Institute, "Second Annual Cost of Cyber Crime Study."

71. Information provided by Manifold, "Project Air Force."

72. Road map provided by Shwedo, "Air Force Targeting Roadmap."

73. Wang, Shisong, and Lin, *Xinxi Duikang Lilun (Information Confrontation Theory)*.

74. Ibid.

75. Ibid.

76. Krekel, Adams, and Bakos, *Occupying the Information High Ground*, 32.

77. Clausewitz, *On War*, 595.

78. JP 5-0, *Joint Operation Planning*, III-22.

79. MCDP 1, *Warfighting*, 46.

80. Ibid.

81. Strange and Iron, "Understanding Centers of Gravity," 9.

82. Ibid., 10.

83. For more examples of what constitutes physical and moral centers of gravity, along with questions to ask to help determine what might constitute moral centers of gravity, see *ibid.*, 11–15.

84. Ibid., 7–16.
85. Ibid., 18.
86. Ibid., 18–19.
87. For full details regarding critical factor analysis and future critical factors, see Rueschhoff and Dunne, “Centers of Gravity.”
88. Wang, Shisong, and Lin, *Xinxi Duikang Lilun (Information Confrontation Theory)*.
89. White, *Medieval Technology & Social Change*, 2–27.
90. Ibid., 2.
91. Ibid., ix.
92. Clausewitz, *On War*, 89.
93. Ibid.
94. Ibid.
95. Kalyvas, *Logic of Violence in Civil War*, 53–54.
96. Deterrence theory is once again referenced as a basis for understanding adversary actions and reactions based on unacceptable threats and credibility of response by a nation or actor. Schelling, *Arms and Influence*.
97. *Chaoplexity* is defined as “the increasing application of computers to the study of scientific problems, the rediscovery of nonlinear mathematics, and an extension of the cybernetic analysis of systems to questions of self-production and self-organization constituted new scientific approaches which crystallized in the theories of chaos and complexity.” Bousquet, *Scientific Way of Warfare*, 34.

Chapter 5

Hypothesizing a Cyber-Power Targeting Theory

To say that strategic theory for cyber power currently is still in its infancy would be a gross understatement.

—Colin Gray
*The Airpower Advantage
in Future Warfare*

Any Air Force which does not keep its doctrines ahead of its equipment, and its vision far into the future, can only delude the nation into a false sense of security.

—Gen Henry H. Arnold

Introduction

This chapter's goal is to focus all previous chapters toward developing a strategic cyber-power targeting theory. To do this, we first must have a common understanding of war fighting. As we strive to develop a theory, the words of Clausewitz are instructive: "Theory should be study, not doctrine."¹ The intent is not to create doctrine or advocate for only one way in which cyber power can be effective, as early airpower advocates did with strategic bombing.

I rely on Clausewitz as an authoritative reference for the understanding of war and warfare, along with other definitions found in US doctrine and established by contemporary authors. Next, an article by Dr. Harold Winton provides a foundation for theory development.² Winton relied upon his reading of Clausewitz to contrive his requirements for a theory. These requirements are provided, along with another deemed necessary by the author, to round out theory development. Finally, a cyber-power targeting theory is offered for USAF cyber efforts, although I believe its value transcends a specific military service and has application at the DOD and national levels.

Since the initial question of this study asks what airpower could offer in developing a cyber-power targeting theory, I argue that the evolution of airpower strategies form a foundation for this theory. Cyber power is in its infancy and has had one central focus on defensive cyber operations, much like

early airpower theorists and studies at ACTS had one central focus on strategic bombing. The challenge to this limited thinking is that it narrows the focus of cyber-power capabilities to a realm that minimizes full-spectrum cyber capabilities in support of combatant commander requirements during war.

Clausewitz stated that battle outcomes are recognized by three distinct signs: “the psychological effect asserted by the commanding officer’s moral stamina . . . , a wasting away of one’s own troops at a rate faster than that of the enemy’s . . . [and] the amount of ground lost.”³ Unless cyber operations are used offensively in all phases of military operations, full capabilities go unrecognized. Using cyber primarily for defensive purposes ignores the dogma that “all war presupposes human weakness, and seeks to exploit it.”⁴ To exploit weakness, offensive action is required.

Today the US military’s cyber efforts appear very similar to the approach of ACTS in the early 1920s. ACTS taught airpower projection through unescorted strategic bombing of industrial capabilities—known as the industrial web theory. The ACTS team, through continued study of warfare and theoretical application of airpower, eventually realized that unescorted bombers required fighter escorts to prevent exponential bomber force losses. The use of combined arms was not new to war fighting, as historical examples of ground and naval warfare abound. In fact, the US Marine Corps built the Marine air-ground task force around the concept of task-organized ground, aviation, combat service support, and command elements. This structure offers commanders a single combined arms force for flexible response.⁵ The Army Air Corps learned valuable lessons with their combined bomber offensives in World War II and thus stuck with the strategy of a combined bomber offensive through the Korean and Vietnam wars. Today’s military cyber-power efforts are generally focused on defensive operations and on supporting other domain operations rather than developing independent offensive and exploitation action. Cyber-power theories should evolve before the next war and consider how full-spectrum cyber capabilities can be used by viewing the enemy as a system.

Warden’s idea of the “enemy as a system” directly shapes the concepts espoused in the cyber-power targeting theory.⁶ It also provides a historical war-fighting theory for airpower that directly correlates to cyber power, although cyber power potentially has a greater holistic effect than airpower alone due to the integration of cyberspace into every aspect of the five war-fighting domains—land, sea, air, space, and cyber. By focusing on the enemy as a system, cyber power can target centers of gravity either independently or integrated with engagements within other warfare domains to bring an expedient end to an adversary’s *capabilities* and *will* to wage war.

It is important to note that during the development of a cyber-power targeting theory, I forgo the argument of whether technology or doctrine should come first in order to build cyber power that is capable of delivering effects. Colin Gray highlights the challenges incurred during airpower theory development while concluding that it is irrelevant whether doctrine or technology comes first, but rather “the focus must first be expanded to encompass the whole of a conflict.”⁷ Just as Gray believes airpower theory should be “conceived, designed, and executed in the context of war and warfare as a whole,” I believe a cyber-power targeting theory should embrace the same context.⁸

Understanding War Fighting: A Foundation to Cyber Warfare

Unfortunately, JP 1-02 does not offer a military definition of war fighting.⁹ To understand how a military capability is used in warfare, the war fighter must understand the concept of war fighting in relation to the conduct of war. For this reason, we turn to US Marine Corps doctrine.

War fighting, as described in MCDP 1, requires an understanding of the nature and theory of war and must be the guiding force behind preparation for war.¹⁰ This should be inherent to any war fighter who understands his or her role and responsibility in protecting national security, while upholding the subservient role of a military as just one *means* to achieve political objectives. Militaries must be prepared to execute in all war-fighting domains when called upon, whether the military is the first or last instrument of power chosen by political leaders.

To execute warfare effectively, military commanders must understand the art of the feasible and the science of the probable in each warfare domain. If commanders know what is technically possible based upon current technologies, they will avoid overpromising on capabilities, as some believe was the case with early airpower efforts and the strategic bombing advocated throughout World War II and beyond.¹¹ Knowing technical capabilities also helps address the perpetual concern Gray says is inherent to literally every dimension of US military power. He states that “US military power is fraught with conceptual uncertainty.”¹² Relative to cyber, Gray argues that “cyberwar [is] bereft of strategic theory tailored for the realms of behavior.”¹³

I posit a different perspective than Gray: US military power is not fraught with conceptual uncertainty about the capabilities inherent to militaries, but rather the use and effectiveness of those capabilities in the next engagement is uncertain. Compound that unknown with the development of new and continually evolving technology, and the proliferation of uncertainty becomes

evident. Clausewitz succinctly identifies these unknown challenges as “uncertainty of information,” or the fog and friction of war.¹⁴

How actors understand war determines how they prepare for hostilities.¹⁵ “What one perceives as the nature of warfare greatly influences the development of doctrine, force composition, and training,” David Lonsdale said.¹⁶ Applying this to the cyber domain, the preparation and employment of cyber power are ongoing in existing military campaigns. Given this fact, it is presumable that cyber power can support traditional conventional force application methods in each of the other domains. But does cyber power stop there? Are we currently employing cyber power as the forward air controller observed ground troop movements for the Army back in the early 1900s? I believe cyber power offers much more than merely being relegated to support roles. It can and should be prepared to act independently, but should not normally be expected to conclude a war on its own. Depending on the effects cyber power can achieve and on the political objectives, in certain cases it is foreseeable that cyber power could conclude a war under the right conditions.

A challenge to military cyberspace operations is the fact that cyberspace is not solely owned by military forces. This is different from all other war-fighting domains in that the employment of bomber aircraft or naval ships operated by military forces does not require collaboration with civilian agencies. However, military forces must collaborate with civilian owned, managed, and operated cyberspace elements in order to achieve effects. This interaction blurs the lines of where military actions begin and end compared to those of civilian organizations and their personnel. It also leads intuitively to examining how adversary war-fighting capabilities are supported by cyber operations to determine where, when, and how friendly forces can affect those capabilities during war without regard to an adversary’s military or civilian lines of coordination. Understandably some will view this as a Douhetian style of “bombing cities and factories instead of military forces,” but that is not the intent.¹⁷ The intent is to focus strategists’ thinking away from just the military forces of an adversary and toward understanding the enemy as a system to aid cyber power target development and planning effects.

Robert Pape suggests that cyber power can be decisive in an engagement by itself, or it can function in a supporting or supported role relative to other war-fighting domains. This will require coordination as militaries must forgo the “loss of institutional autonomy” to maximize military effectiveness.¹⁸ The interoperability of cyber power with other military—and civilian—instruments of power is relatively unknown and untested but that should not inhibit thinking about how to improve its capabilities. Unlike Pape’s argument that threats to civilians by airpower are wasteful and immoral, I argue that military cyber

power is wedded to countless civilian cyberspace operations and therefore requires civilian inclusion when determining threats and threat response actions—or “sticks and carrots.”¹⁹

When someone claims that a single war-fighting domain can function independently and win a war, we should question the validity of their assertion. Past wars clearly show this is not the case. However, each domain must be prepared to operate independently, as well as collectively, when called upon. Since most future wars will probably be limited in nature, the military is unlikely to employ full military capabilities from the onset of war through its conclusion, no matter how much a commander desires this. Escalation from low intensity (limited war) toward high intensity (total war) appears likely, rather than the days of planned engagements on the battlefield where opponents met and a clash ensued until a decision was reached.²⁰

If escalation is how future war fighting will evolve, as opposed to the sudden onset of total war, then militaries must ask themselves how they are preparing for warfare in cyberspace. How are US military cyber forces preparing to respond to calls for national-level cyber power application, especially when the United States has not defined what constitutes cyber war or cyber warfare? More directly, how is the USAF preparing for the strategic use of cyber power? Do cyber warriors understand the nature and theory of war to guide preparations, as MCDP 1 requires? Will a cyber-power targeting theory aid the development of doctrine, force composition, and training as Lonsdale suggests?

Determining whether cyber warriors understand the nature and theory of war is beyond the scope of this work. Since the focus is on the Air Force, the scope is limited to the chain of command for Air Force cyber operations. It is safe to presume that commanders of US Strategic Command, USCYBERCOM, and Twenty-Fourth Air Force understand war-fighting concepts. What may be missing is the national institutional support required to prepare their forces for cyber warfare. Doctrine is in its infancy, organizational roles and responsibilities are still being fleshed out, and combat experience in cyber warfare is minimal.

It is important to note that doctrine supports operations; it does not dictate or control them by establishing limiting parameters. MCDP 1 states that “doctrine must continue to evolve based on growing experience, advancement in theory, and the changing face of war itself.”²¹ Given the fact that cyber warfare has not occurred overtly, mainly because the United States has not clearly defined what constitutes cyber war, the USAF has minimal open-source experiences for developing cyber doctrine. Waiting for doctrine to drive military and domestic security of the cyber domain, as General Arnold suggests in the opening quote, is not an option. Actions are required to protect

and defend cyberspace today if the United States intends to maintain superiority in all war-fighting domains while protecting the nation's most vital security interests. The following principles and proposed theory are intended to provoke thought and action about future US Air Force war fighting in the cyberspace domain, as well as cyber power projection in all war-fighting domains.

Recalling the Principles of War and Applying Them to Cyber

The application of cyber power must be guided by longstanding principles of war regarding force application. Just as military power is projected in the other four domains—land, air, sea, and space—military power can be projected in cyberspace. This review of the principles of war will enable the reader to digest the standing principles and invites critical thinking regarding a proposed cyber-power targeting theory.

AFDD 1 describes the principles of war for airpower: unity of command, objective, offensive, mass, maneuver, economy of force, security, surprise, and simplicity.²² These principles should “serve as valuable guides to evaluate potential courses of action” and not as a “checklist to guarantee victory.” With this in mind, recent wars have caused the Air Force to develop four additional principles: unity of effort, restraint, perseverance, and legitimacy.²³ As cyber warfare evolves, it is incumbent on the practitioners and strategists alike to espouse new principles when required.

The challenge for cyber power today, as it was when airpower was initially evaluated for military use, is to overcome initial barriers to efficacy in order to achieve warfare objectives in support of political *ends*. I focus on the traditional principles of war and rely upon the works of Dr. Sanu Kainikara to briefly explain each one (table 5.1).

Table 5.1. Principles of war

Principle of War	Principle Defined	Espoused by Theorist
Objective	The single path to success in aerial warfare is unwavering adherence to the principle of <i>objective</i> . The adaptability of air forces to many missions and the ease with which they may be diverted encourage vacillation and defeat.	General Air Force Principles' Lecture, Air Corps Tactical School, 1934–35
Mass	The principles of war could, for brevity, be condensed into a single word: concentration.	B. H. Liddell Hart, 1930s
Offensive	Air forces characteristically take the offensive. Even in defense, they defeat an invading enemy by attack.	AU Manual 1, <i>USAF Basic Doctrine</i> , 1951

Table 5.1. Principles of war (continued)

Principle of War	Principle Defined	Espoused by Theorist
Security	Always presume that the enemy has dangerous designs and always be forehanded with the remedy.	Fredrick the Great, 1740–1786
Surprise	I believe that, more or less, all of the Allied operations [in the Southwest Pacific] depended on deception by landing in places where we thought a landing and the building of airfields impossible.	Lt Col Masaru Shinohara, Japanese Eighth Area Army, 1942–1967
Maneuver	An air force commander must exploit the extreme flexibility, the high tactical mobility, and the supreme offensive quality inherent in air forces to mystify and mislead his enemy and to threaten his various vital centers.	J. C. Slessor, 1943–1952
Economy of Force	To me an unnecessary action, or shot, or casualty, was not only waste but sin.	T. E. Lawrence, 1914–1935
Simplicity	Avoid unnecessary complications in the planning, organizing, and conducting of military operations.	S. Kainikara, 2011
Unity of Command	Subscribes to the airpower tenet of “centralized control and decentralized execution.” This is also evident in the single component commander theory for like forces within an area of responsibility.	S. Kainikara, 2011, and author’s interpretation of the JFACC role

Created by author based on Sanu Kainikara and RAAF Air Power Development Centre, *Principles of War and Air Power* (Tuggeranong, Australia: Air Power Development Centre, 2011), 6.

Kainikara provides an excellent synopsis of standing principles of war derived from the study of Sun Tzu and Clausewitz. As he suggests, principles of war are the primary guiding elements in the conduct of conflict enshrined in a nation’s doctrine, which normally only changes when radical shifts in national security priorities occur.²⁴ Each principle of war has a role in projection of airpower.

Though we cannot dissect how the principles of war guide the conduct of cyber war, mostly because of a lack of real-world experience, some principles of cyberspace operations are beginning to circulate within the cyber community. Maj Gen Brett Williams developed 10 propositions regarding cyberspace operations while serving as the Pacific Command/J6 in Hawaii (table 5.2).²⁵ These and other principles regarding cyber power are critical and required; however, it is relevant to understand the context of each. General Williams focuses on what he calls the operational level of war fighting as he espouses control of cyber forces and operations during war by the combatant commander. My concern is that cyberspace is not confined to a region, despite General Williams’s push to construct the global information grid accordingly. Therefore, giving control of cyberspace to a joint force

HYPOTHESIZING A CYBER-POWER TARGETING THEORY

commander (JFC) might have unintended consequences for a JFC in a different region. General Williams's perspective depends on the context of the combatant commander at that time and does warrant analysis in order to enhance JFC operational cyberspace capabilities.

Table 5.2. Ten propositions regarding cyberspace operations

Propositions	Author's questions to provoke thought
Cyberspace is a war-fighting domain. At the operational level of war, cyberspace operations are most similar to those in land, maritime, and air.	Does cyberspace afford capabilities to multiple JFCs operating in diverse regions? A soldier, naval vessel, or an aircraft can only be in one location at a time; cyberspace in one theater can support operations in multiple theaters simultaneously.
The JFC must have C2 [command and control] of cyberspace, just as he does of the terrestrial domains.	Would a national-level cyber tasking order allow the JFC a medium for executing cyber targeting objectives? Will a higher-level tasking process afford limited assets (i.e., cyber force operators) to conduct more missions on a broader scope?
C2 of cyberspace is the key enabler for exercising operational command and control.	Does C2 at a higher echelon than the JFC make sense so that situational awareness across the entire global information grid is understood before a regional JFC executes a cyberspace operation that might affect other regions/operations?
Defense is the main effort in cyber at the operational level of war.	Is defense the main effort for cyber during war, or does the main effort become offense? If offense, should that be the main effort during peacetime as well so OT&E is geared toward wartime objectives accordingly?
Cyber is the only manmade domain. We built it; we can change it. Creating a cyber JOA [joint operating area] is the first requirement.	Does this move cyberspace back to days of different operating standards for different forces across the combatant commands?
Cyberspace operations must be fully integrated with missions in the physical domains.	Are barriers to this integration the current security practices, exercise limitations, or lack of capable cyber forces necessary to integrate full spectrum warfare operations? How do nonmilitary capability providers enable or prevent full integration since unlike air, land, or sea, US forces do not own the entire cyberspace infrastructure required to create the desired effects?
The JFC must see and understand cyberspace to defend it—and the commander cannot defend it all.	Will automated sensors with passive and active defense systems enhance JFC confidence? Can these be managed from a national level with a local detachment providing instant data to the JFC to meet this intent?
Networks are critical and will always be vulnerable—disconnecting is not an option. We must fight through the attack.	When comparing cyber to the traditional domains (land, sea, and air), are there times where cyber forces must retrograde or retreat? Should this remain an option for cyberspace operations as well or is unplugging the possible solution in order to prevent a complete loss of warfare objectives or salvage national security interests?
Our understanding of nonkinetic effects in cyberspace is immature and effects created through cyberspace are not solely nonkinetic.	Can virtual ranges, increased real-time cyber operations in recurring exercises, and use in real-world operations grow this understanding? Can the cyber community reduce security constraints within the military community in order to increase lines of communication and understanding between cyberspace capabilities and those of other warfighting domains?
Understanding operational impact is the critical measure of cyberspace engagements.	Does this impact include the readiness of cyber forces through military OT&E actions as well? Is there value in conducting “days without cyber” to test the operational environment during peacetime to better understand potential impacts during combat?

Reprinted from Brig Gen Brett Williams, “Ten Propositions Regarding Cyberspace Operations,” Joint Force Quarterly 61 (2nd Quarter 2011): 10–17.

Cyberspace as a War-Fighting Domain

Another issue to resolve before defining a cyber-power targeting theory is the identity of cyberspace as a war-fighting domain. This domain is not readily accepted by all, including academics such as Martin Libicki. Libicki concludes that the “null hypothesis”—that cyber power does not matter—remains to be disproved.²⁶ I reject that argument and find the debate academic in nature and futile in moving military cyber power forward. In fact, testing to determine if cyber power matters or not is irrelevant—cyber power is important. The questions we should ask are, what impacts can an adversary’s cyber power have on US vital interests, and how should US military forces be postured to meet security and political objectives? The focus of Libicki’s argument should be on evaluating adversaries’ vulnerabilities to cyberspace operations, while identifying friendly critical capabilities and vulnerabilities that must be protected in war given the growing operational reliance on cyberspace.

Cyberspace operations pervade every conventional war-fighting domain. Cyberspace not only enhances current operations, but new technologies push greater interconnectedness more each day. This domain not only affects military operations, it also impacts the very soul of the United States’ capitalistic society. In banking, logistics, navigation, air traffic control, electric grids, and much more, the cyber domain is embedded in diverse operations enabling society to function more efficiently each day. Maj Gen Suzanne Vautrinot, Twenty-Fourth Air Force commander, pithily describes the cyber domain as “an environment of intellect, integration, and, for good as well as ill, complex interdependency.”²⁷

The United States cannot ignore cyberspace as a war-fighting domain; it must employ lessons learned throughout history while not being blinded by cognitive dissonance. The nation’s security requires military forces to recognize the new opportunities cyberspace affords protectors of freedom. Creating a cyber-power targeting theory requires an understanding of cyberspace and the cyber domain. Accepting or rejecting cyberspace as a domain will either coalesce or divide thinking by strategists and tacticians. In the United States, such thinking must coalesce as the nation prepares for future war.

Stuart Starr, in “Convergence of Sea Power and Cyberpower,” suggests that there are 28 possible definitions of the term *cyberspace*—but in reality, it requires only one.²⁸ This study uses the National Defense University’s definition: “Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Inter-netted information systems and their associated infrastructure.”²⁹ There is one

element to add to this definition—the human element. Cyberspace also includes all human elements that create, interact, disseminate, and negate information or the system itself in, through, or from cyberspace. Since cyberspace is a man-made domain, the human element is critical to an inclusive definition.³⁰

Cyberspace is a domain equal to air, land, sea, and space. A domain is “a territory over which dominion is exercised.”³¹ I posit that dominion within cyberspace is probable and already evident. Stuxnet—the cyber attack on Iranian centrifuges—would not be possible without operations in the cyberspace domain.³²

Militaries desire the ability to dominate in cyberspace despite the “Wild West” syndrome.³³ Given the limited battleground in which cyber power has been wielded in the real world, many benefits of operating in the domain are speculative at best. Starr acknowledges some of these benefits, stating that accepting cyberspace as a distinct domain will have significant implications for equipping cyber forces and developing a culture for cyber activities.³⁴ This sounds eerily familiar to early airpower supporters who advocated a separate service before 1947. In fact, we are again talking about a new type of military power, one that can have devastating effects in war just as air, land, and sea power can. To be effective, strategists must think about employing a weapon system while striving to understand its effects on the adversary and on meeting political objectives. Theory is a tool to encourage this thinking. One upfront challenge to creating cyber theories of any kind is the limited experience with the subject of *theory* espoused by Clausewitz.³⁵ However, that cannot be justification for not trying to develop something useful.

Basis of Theory Development, Wintonian Style

This study suggests a cyber-power targeting theory for military cyber power application in war. Scoped to the perspective of Air Force cyber power, I hypothesize that the propositions are applicable to DOD and national-level cyber war objectives. Development of a military theory is achieved by employing the Wintonian model, which claims that the theory defines, categorizes, explains, connects, and anticipates.³⁶ Relating definitions to their importance in cyber targeting is the first step in *defining* cyber targeting. At the same time, we must understand cyber targeting’s importance to war fighting. The cyber-power targeting theory continues to evolve by *categorizing, explaining, connecting, and anticipating* the use of cyber power as a military instrument of power by focusing cyber targeting efforts on suggested centers of gravity.

I add a final aspect of theory development—a *testing* phase—to the cyber theory. This additional step goes beyond Winton’s theory model but is critical to determining a theory’s worth. Since the intent of war is to compel an enemy to do one’s *will*—and accepting Clausewitz’s assertion that military operations are subservient to political objectives—the strategist must understand the limits of force and know when political objectives are beyond the reach of military action.³⁷ Until a theory is tested, its true worth is subjective; waiting to test it in warfare is undesirable, although warfare provides more valid information than preconditioned exercises and testing.

Clausewitz suggests that “theory should be study and not doctrine”; however, if the Air Force does not think about cyber doctrine and operational tactics, techniques, and procedures now, then it may be in the same situation airpower forces were in before World War I.³⁸ Because the United States did not have adequate knowledge of military aviation, “the military had to improvise and depend on allies for advanced training of the Air Service.”³⁹ If the USAF develops a cyber-power targeting theory and tests it in both real-world and exercise scenarios, then applicable doctrine with supporting operations such as OT&E functions can be established. Developing a foundation for cyber power in warfare will enhance coordination with other military services, civilian agencies, commercial industries, and allies. These foundations can expand as additional experiences are gained.

Developing a Cyber-Power Targeting Theory

It is important to remember Winton’s sage advice before developing a theory: “no theory can fully replicate reality . . . and military theory practically always lags behind the explanatory curve of contemporary developments.”⁴⁰ He described a few key attributes to consider when developing a theory. First, one must *define* the field of study under investigation, just as Clausewitz defined war.⁴¹ Unlike Clausewitz, who had both history and experience in warfare, theorists have no experience of cyber war. We will first discuss the definitions of cyberspace, cyber war, and cyber attack and then develop cyber targets to help shape a theory.

The second task is to *categorize*. Clausewitz’s premise that wars can be offensive and defensive is applicable to cyber power targeting and will be used to develop the theory. Exploitation will also be added as a third category in which cyber operations can and are being conducted by various nations and individual actors.

Third, Winton claims that “*explanation* is the soul of theory,” and I agree. Developing a cyber-power targeting theory will facilitate an open dialog regarding military expectation and the use of cyber power. I also hope that defining the specific roles of cyber power will lead to the development of US policy regarding cyber attacks, thus creating domestic and international standards of behavior in cyberspace.

The fourth objective is to *connect* cyber operations to other military domains in order to integrate the newest war-fighting domain and its capabilities into established concepts of operation. This study will potentially highlight gaps between civilian and military roles and responsibilities in cyberspace operations, as well as cyber vulnerabilities of critical national infrastructure, thus pressing the need for an overarching US organization to manage cyberspace. This “Department of Cyber” would be supported by USCYBERCOM, much like US Northern Command supports the Department of Homeland Security.

A fifth aspect of theory development is to *anticipate*. “Anticipation can be almost as useful as prediction,” said Winton, arguing that action and reaction in the human arena are less definitive.⁴² Given the undefined parameters of what constitutes cyber attacks and the lack of cyber war up to now, any cyber-power targeting theory is going to fall into the realm of anticipation. My intent is to anticipate how defining cyber attack and targets the United States values as critical to national security might dissuade further attacks by publicly acknowledging an intended US response to such threats.

The sixth and final factor in this theory, one I added, is *testing*. Although no cyber war has occurred, there have been conflicts in which cyber attacks were possible and did in fact occur. In conflicts where cyber power was not used or not known to the public, the question is, why not? Are cyber attacks limited by the lack of policy and authority given to military commanders, thus limiting the military instrument of power? I believe that cyber power is just another arrow in the quiver. Although cyber power is a new capability, it is not a nuclear weapon; therefore, should we be guarding its capabilities like they are nuclear weapons? Given the porous nature of cyberspace, would US interests be better served through demonstration to establish credibility upon which to build deterrence? A review of the Stuxnet attack will be used to demonstrate my intent.

Define

The occurrence of a cyber attack seems to be daily news. The topic has been somewhat obscure for the past decade, but with hacking stories becoming

more prevalent in news sources such as the *Wall Street Journal*, *Washington Post*, and *New York Times*, suddenly there is plenty of press on the subject.⁴³ This is to be expected in a world filled with what Dave Grossman calls sheep, wolves, and sheepdogs. Grossman says the sheep (society) pretend the wolf (enemy) will never come, but the sheepdog (military—defenders of society) lives for that day. That day is already upon the United States in regard to cyber war.⁴⁴ The question is, what is the United States going to do about it?

“If a terrorist group does obtain destructive cyber weapons, it could strike with little hesitation,” senior leaders like William Lynn, US deputy secretary of defense, warn.⁴⁵ Secretary Lynn, while not necessarily a sheepdog, is creating anxiety within cyberspace, a realm the sheep of most societies view as non-threatening. He is also awakening the sheepdog (the military) to problems that have been watched for some time, but offensive military response has not yet been warranted and will not be until the sheep support such actions. However, challenges still exist, which prevent a military response short of declared war.

First, the United States has not defined what constitutes a cyber attack. Second, US policy makers have not publicized what type of cyber attack calls for a military response, using either military cyber capabilities or another US military instrument of power. The second point is important for any USAF cyber power response, although it does not prevent the service from building capabilities to respond when called upon. The USAF could prepare more effectively with objectives defined clearly by the policy makers. For that reason, defining what kind of cyber attack warrants a military response is required.

The rhetoric espoused in the *Department of Defense Cyberspace Policy Report* stating that the Obama administration “will respond to hostile acts [against the United States] in cyberspace as we would to any other threat to our country,” does nothing to clarify or define a cyber attack.⁴⁶ Neither do books such as *Cyber Attacks* by Edward Amoroso, which highlights potential vulnerabilities of US systems and describes what steps can be taken to mitigate known vulnerabilities.⁴⁷ To hone a definition of what constitutes a cyber attack, we must zero in on what is critical to US national security. We must also acknowledge the fact that it is “the public, the civilian population of the US, and the publicly owned corporations that run our key national systems, that are likely to suffer in a cyber-war,” as Richard Clarke alludes to in *Cyber War*.⁴⁸ Clarke’s definition of cyber war—actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption—can shape a US definition of cyber attack, at least in relation to conflict between nation-states.⁴⁹

There is still no clear standard about what constitutes a cyber attack; no formal definition exists. However, evaluating the United Nations (UN) charter

leads to the conclusion that the use of force would include cyber attacks since it is a domain for warfare just as air, land, sea, or space.⁵⁰ Article 51 of the UN charter allows for the right of self-defense; however, the International Court of Justice (ICJ) has set a high bar to exercise the right.⁵¹ Many cyber actions may not meet the ICJ standard, but Article 39 of chapter VII states the UN Security Council “shall determine the existence of any threat to peace, breach of the peace, or act of aggression and make a recommendation.”⁵² Any recommendation made by the Security Council falls under Articles 41 and 42 of the charter. Article 41 covers nonmilitary responses, whereas Article 42 allows military response using land, air, or sea forces.⁵³ Thus, the door is open for a potential military response to another country’s aggression via cyber attack.

A nation claiming to be harmed by a cyber attack by another nation-state that did not rise to the level of an armed attack could make its claim to the UN. The UN Security Council would evaluate such a claim and determine if a response using force is warranted, just as it currently does for the other three authorized warfare domains—air, land, and sea. Using inductive reasoning, and because the UN charter has yet to include cyber war or define what constitutes a cyber attack, “cyber” can be added as a domain in which a response under Article 42 or 51 can be conducted. But there is still no clear standard as to what constitutes a cyber attack, nor does the speed at which cyber attacks occur allow for the time needed to gain approval from the UN in order to quickly respond.

It is safe to presume that the UN will legally review each war, as it has done for every war or conflict that has concluded since the organization was founded in 1945.⁵⁴ Lawyers will review actions before war—*jus ad bellum*—as well as actions in war—*jus in bello*.⁵⁵ Legal literature about cyber attack may help identify a usable definition of a cyber attack that would constitute an act of war. Matthew Waxman in the *Yale Journal of International Law* provides a starting point. He defines cyber attacks as “efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them . . . encompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term).”⁵⁶

There are endless possible targets for a cyber attack, given the pervasive interoperability between cyberspace and the countless operations conducted within society each day as well as the many nefarious actors conducting cyber attacks. Since the scope of possible targets within the United States is much too broad for US military forces to focus on, it is important to focus on threats to US national security for our discussion and theory development.⁵⁷

Interests involving national security can be derived from published grand strategy guidance such as the *National Security Strategy*. This strategy, signed by President Obama in 2010, currently informs the international community about US interests and identifies four enduring national interests:⁵⁸

1. Security—the security of the United States, its citizens, and US allies and partners
2. Prosperity—a strong, innovative, and growing US economy in an open international economic system that promotes opportunity and prosperity
3. Values—respect for universal values at home and around the world
4. International Order—an international order advanced by US leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges.⁵⁹

This study's focus on Air Force cyber operations requires a look at the Air Force vision intended to meet defined national objectives. Gen Mark Welsh, chief of staff of the Air Force (CSAF), described today's Air Force vision in terms of five roles and responsibilities that have been inherent since the Air Force was founded in 1947: air and space superiority; intelligence, surveillance, and reconnaissance; rapid global mobility; global strike; and command and control.⁶⁰ We could make one addition to the first role and responsibility in the CSAF's vision—"air, space, and *cyberspace* superiority"—which would include the three primary roles defined in the Air Force mission to "fly, fight, and win . . . in air, space, and cyberspace."⁶¹ This is also in line with the fiscal year 2013 *Air Force Posture Statement* published in early 2012.⁶²

A review of the posture statement leads to a second change in the current vision by General Welsh; I add "nuclear deterrence" as a sixth primary role and responsibility. There are additional focus areas within the posture statement that are important to national security and susceptible to cyber attacks, but I chose to focus on six primary roles and responsibilities because this paper is limited to developing an Air Force cyber-power targeting theory. These roles are: (1) air, space, and cyberspace superiority; (2) intelligence, surveillance, and reconnaissance; (3) rapid global mobility; (4) global strike; (5) command and control; and (6) nuclear deterrence. If the Air Force decides these six areas are critical to airpower operations and should be protected from an adversary's cyber power capabilities, these may be enemy centers of gravity to exploit, presuming the adversary is a peer competitor with the United States.⁶³ Accepting this inference is in keeping with Clausewitz's and Warden's principles of defining enemy and friendly centers of gravity before war.

Categorize

Six definitive cyber power targets result from clearly defining *cyber attack* and the six critical capabilities are levied upon the USAF to protect both defined national security vulnerabilities and military power in support of national security interests. These targets will shape Air Force cyber operations in the form of offensive, defensive, and exploitation initiatives.

From an offensive and defensive perspective, USAF cyber forces must conduct both active and passive operations to prevent adversary attempts to alter, disrupt, or destroy any computer system, network, information, or software program associated with the six defined roles and responsibilities. These efforts require coordination with other military services, civilian agencies, and allies in order to guarantee the capability of each Air Force mission. Ongoing cyber exploitation initiatives during peacetime and war are necessary to ensure cyberspace freedom to maneuver exists when needed.

To deter adversary aggression in these areas, US policy makers should establish policy stating that any cyber attack on these assigned Air Force roles and responsibilities will be considered an act of aggression. This same policy effort should be done for all areas of national security interests; however, the focus remains on the Air Force for this study. The policy should also state that cyber attacks deemed acts of aggression will be met with an immediate response by the appropriate instrument of power as determined by policy makers. Publishing this policy would be a first step in establishing both domestic and international standards—or a code of conduct—within cyberspace, potentially acting as a deterrent.

Establishing a defined policy regarding cyber attack, in addition to the already stated Air Force mission of cyber superiority, also enables the creation of cyber targets for offensive cyber operations. Reflecting on what the Air Force deems critical to mission success, an inverse look at similar capabilities of an adversary identifies potential centers of gravity for cyber attack by US forces. Finding, fixing, tracking, targeting, engaging, and assessing roles are just as critical in cyberspace operations as they are in land, air, and sea warfare. If anything, cyberspace operations require more intelligence gathering and verified updates than any other domain, with the higher probability of being wrong. This is due to the expedience this man-made domain makes when compared to other domains.

Gen Bradford Shwedo, director of intelligence, Headquarters Air Combat Command, said that “cyber is an Intel hog.”⁶⁴ His point hinges on a few key differences regarding intelligence gathering, consolidation, processing, and then supporting ongoing and future operations. He acknowledges the well-

known OODA loop of Col John Boyd and postulates that this loop is defined as “operate, attack, exploit, defend” in cyber operations.⁶⁵ This loop is applicable in the offensive, defensive, and exploitation objectives of Air Force cyber operators.

Clausewitz states that the characteristic of war may be split into two main categories: preparations for war and war proper.⁶⁶ I agree with the premise that offensive and defensive cyber operations are primarily war proper activities with some aspects conducted during preparations for war, whereas cyber exploitation is a preparation for war activity with some aspects conducted during war proper. It is also important to point out a point contrary to Clausewitz. Clausewitz said that “defense is the stronger form of combat.”⁶⁷ His point is relative to maintaining the physical forces of a country; if those forces are lost, then the country is lost automatically. This is not the case with cyber operations. Libicki substantiates why offensive cyber forces must be actively engaged and active adversarial capabilities must be destroyed, disabled, or otherwise inhibited.⁶⁸ “In cyber, offense is cheap and can have disproportionately great effects at the levels of attack—advantage attacker,” he said.⁶⁹ Therefore, offensive cyber power is vital.

Offensive cyber operations are arguably the strongest form of warfare in cyberspace. Cyber warfare is a cunning tool in war given the diverse nature of cyberspace and the way in which it allows operations to rapidly move from one location to the next. Unless you remove the true genius of its ability—the human operator—the defensive battle as the stronger form of warfare appears incompatible with the cyberspace domain. Offensive operations, both nonkinetic and kinetic, must take priority for cyber operations. Depleting aircraft, aircraft carriers, tanks, and even soldiers can aid in determining an adversary’s war-fighting capabilities. Determining where the shadowy cyber forces are operating is difficult, making it hard to destroy the true capability of cyber power. The complexity of operating in this domain, under the current incoherent policies governing military operations, is evidenced in the fight against al-Qaeda and foreshadows what is ahead in the battle for cyberspace. In 2010 Gen John Abizaid concluded that in the war against al-Qaeda “cyberspace is a domain of war where you have to conduct defensive and offensive operations. The enemy was moving in the cyberspace world in a way that allowed them to recruit, train, organize, equip, proselytize, educate, and conduct intelligence operations.”⁷⁰ Because cyber forces can literally operate around the globe instantaneously, cyber warfare is much more complex than war fighting in any other domain.

Thus there is a clear delineation between the cyber domain and the other war-fighting domains. Knowing the enemy’s offensive disposition in cyber is

virtually impossible. Even if a lack of enemy capabilities exists before war begins, once war starts intelligence can quickly assess the adversary's number of ships, airplanes, and even fighting forces in brigade formation. Enemy capabilities are not easily identifiable in cyberspace. This is exactly why offensive cyber operations cannot be relegated to tit-for-tat operations or be used solely as combat air support for fielded forces as airpower was originally. Cyber operations place military operations back in an attrition style of warfare and require that military cyber forces focus more on offensive operations than defensive, at least on the war continuum spectrum.

Offensive cyber can assist air, land, sea, and space forces in achieving their operational requirements. But to be the most effective, offensive cyber should target strategic capabilities that aid political objectives to bring about quick conflict resolution. Employing Warden's model of the enemy as a system and targeting national command and control capabilities, key processes, infrastructure, the population, and fielded forces seem to be the most efficient method in which to employ cyber power, at least theoretically. DOD and specifically Air Force cyber forces must be prepared to conduct simultaneous offensive cyber operations targeting each center of gravity of the enemy's systems. Obviously these efforts must coordinate actions with those in other domains to ensure synergy is achieved. However, there is little doubt that cyber will be the first salvo fired in future wars.⁷¹

Cyber defense is arguably conceptually different than other warfare domains. The US Navy defends the littoral territorial boundaries; air defenses, either through missile defense initiatives or alert aircraft, define airspace boundaries. Those lines are not readily identifiable in cyberspace. Susan Brenner acknowledges that traditional attacks from the territory of one nation-state upon another presumptively constituted an act of war.⁷² She claims that the contemporary territorial boundaries are antiquated parameters in determining cyber threats. The question is why? People still reside in a sovereignty, and if a cyber threat affects a society in which they live, no matter what form an attack takes or what domain it originates from, why treat it differently? Until the international community develops a standard for cyber threat resolution, a formal US policy that states US intentions to respond to cyber threats should serve as the applicable law and warning. Such a law should apply to US citizens living within the territorial boundaries of the United States as well as non-US citizens living within the US borders. Those who break the stated laws should pay the consequences. This is no different than domestic laws. Either people respect them and avoid penalty and punishment or choose to disobey them and reap the applicable consequences.

Defensive cyber operations appear to be the primary focus of Air Force cyber operations today, as well as across DOD and civilian cyber efforts. Automated host base security system efforts that report vulnerabilities through automated scripts, passive defense protocols, and ensurance that the latest antivirus software is loaded on government computers are all very costly efforts. In reality, they are all reactive security measures that do little more than provide a false sense of security to the average cyberspace user. They are useful but only to a point.

Zero-day exploits by those who initiate cyber attacks are not deterred by signature-based antivirus software programs, which today's antivirus software updates are based on.⁷³ Attackers know it will take an average of nine months or more before any new virus protection will identify the exploit they create. Then software owners must actually get the software updates—something that does not occur automatically—to close the vulnerabilities.⁷⁴ That allows for a lot of maneuverability in cyberspace for an adversary. The damage sought is most likely done within nine months of an attack, or additional unknown vulnerabilities are planted in other cyber systems that can be executed at the adversary's choosing.⁷⁵ These are the same attackers who are actively seeking software vulnerabilities and creating "logic bombs" to exploit vulnerabilities without being detected.⁷⁶ They are well versed about when antivirus script updates occur and which vulnerabilities have been closed.

Given the unlimited vulnerabilities to DOD networks and the fact that the DOD does not own its own infrastructure, develop its own software programs that govern all military needs, or provide maintenance for its end-to-end cyber systems that support defined national security objectives, a change in DOD and specifically Air Force defensive cyber operations is required. The focus must shift from trying to protect all Air Force and DOD cyberspace to one that guarantees protection of the cyberspace that is critical for national defense and national security strategic objectives. In other words, the six roles of Air Force cyber power targeting defined above become the primary focus of Air Force cyber defense operations for cyber forces. The primary job of Air Force cyber forces is to conduct relentless protection of those capabilities to assure mission success when these capabilities are called upon.

The proposed concept might push militaries to operate in two distinct cyberspace domains—open versus closed—for both security and operational reasons. Elihu Zimmet and Charles Barry argue there are two broad cyberspace regimes that require different attributes. The first is an open network that aids collaboration, information sharing, and situational awareness.⁷⁷ The second is a closed, secure network in which speed of operation, assured delivery, and integrity of information are vital.⁷⁸ As an experienced cyberspace operator,

the closed network is most appealing for mission assurance. However, military forces must also operate in the open network to interact and collaborate with allies and exploit adversary vulnerabilities. Military commanders must advocate the right balance, based on cost/benefit analysis and acceptable risk tolerance, between mission assurance and offensive and exploitation actions in a contested cyberspace.

The last category for Air Force cyberspace operations is exploitation. Authors such as Thomas Rid of King's College London argue "cyber war will not take place."⁷⁹ In addition to stating cyber war has never happened and is highly unlikely to occur in the future, Rid claims sabotage, espionage, and subversion are not cause for war. This fallacy is based on the lack of a defined nation-state policy and established international laws. My argument is that once the United States defines such acts as illegal, they become acts of aggression that can lead to war. However, this approach needs some common sense. I draw a distinction between actions conducted in open-source cyberspace (unprotected or inadvertently made public information is fair game and is not illegal) and those carried out in closed network systems (circumventing security protections or hacking into non-open source systems), which leaves room for espionage-type activities. This is no different than human intelligence activities that gather information through social engineering or observation techniques.

These open-source activities are not to be confused with active deceit. Exploiting the weakest part of the infrastructure—the people—by sending a phishing e-mail with an embedded executable file would be considered an act of low-threat aggression.⁸⁰ However, requesting that users complete online surveys or other persuasion techniques to get users to relay information would not be. Any user who knowingly provides sensitive information would constitute a failure of internal processes, procedures, and training.

Exploitation efforts require enormous intelligence gathering resources to help shape the cyber operator's focus. The starting point for exploitation efforts would be equivalent adversary capabilities for the six Air Force cyber power targeting roles identified. From there, defined centers of gravity of a potential adversary in regard to cyberspace reliance would shape US espionage efforts. Any function that supports the enemy's strategic systems would invariably become exploit areas of interest. Understanding the interconnectedness of the systems; finding vulnerabilities at choke points where data flows; and relying on consolidated power sources, or cloud data storage facilities, intelligence collaboration centers, or combined area processing centers for

logistics, banking, agricultural, or other crucial functions also become critical. These exploitation efforts must be constantly coordinated with offensive and defensive actions within military and nonmilitary agencies. Coordination can avoid redundancy and waste, synchronize efforts against a target, and lessen the possibility of fratricide to friendly cyber operations.

Explain

As mentioned, the military is one instrument of national power that serves the political objectives of policy makers. For that reason, military commanders are constantly aware of threats to national security that presumably many members of society either do not notice or choose to ignore. Recall the sheep discussion from Grossman earlier. Until societies realize a threat and push elected officials to resolve that threat, military and other federal agencies are limited in threat response actions. Responding to cyber threats is no different.

In 2012 Congress lobbied for legislation that would allow the National Security Agency to share its sophisticated cybersecurity tools with the corporate sector. That legislation was opposed by the US Chamber of Commerce.⁸¹ In early 2013, after an onslaught of “distributed-denial-of-service attacks” and new “swarm” attacks on “the soft underbelly of American society,” the private sector requested government help to thwart attacks.⁸² It appears to be both an opportunity for the civilian sector to strengthen its cybersecurity capabilities and for the military and other federal agencies to test offensive and defensive capabilities to counter growing threats. It is also a prime time for policy makers to establish acceptable cyberspace behavior standards before more precedent is set by not condoning or responding to cyber threats.

Operating in the vulnerable sectors of a nation’s cyberspace—before war is declared—can be considered phase 0 military operations. Explaining each phase of military operations—without delving into tactical offensive, defensive, or exploitation specifics—invites critical thinking about when and how cyber effects might be employed.

Pundits argue that “phase 0” is new to the military lexicon, whereas phase 1 to phase 5 operations are traditional military roles substantiated in existing doctrine.⁸³ This may have been true years ago, but it is an antiquated argument today. If we turn to joint doctrine for an understanding, JP 3-0 clearly shows six phases of military operations (fig. 5.1). The figure succinctly captures traditional military endeavors during each phase.

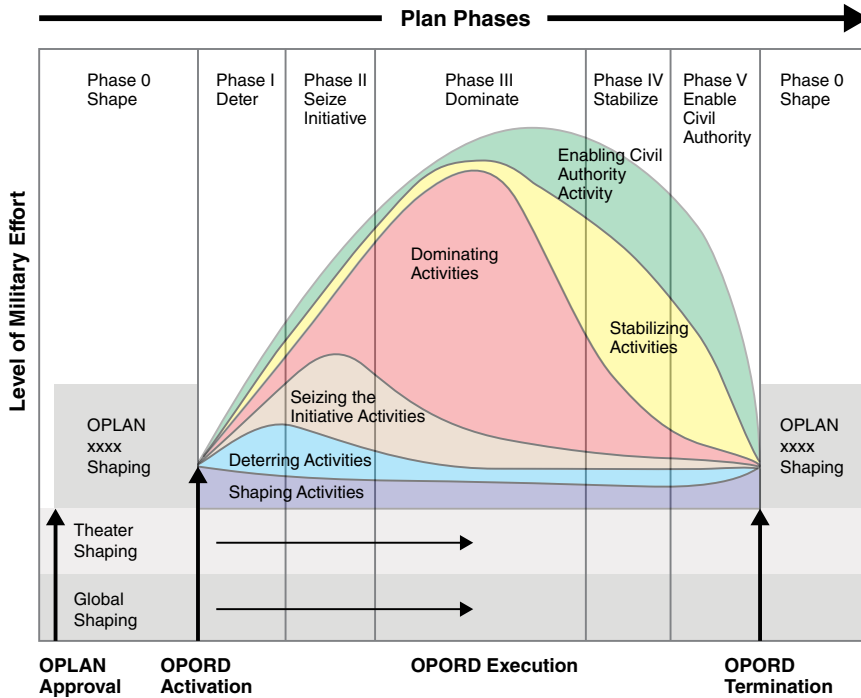


Figure 5.1. Military phases of operation. (Reprinted from JP 3-0, *Joint Operations*, figure V-3, "Notional Operation Plan Phases," V-6.)

I suggest that shaping operations in cyberspace are ongoing throughout the entire pendulum of peace to war and back to peace again. I do not intend to suggest that aggressive military operations in cyberspace are always required during times of peace but rather that shaping the cyberspace sphere inevitably occurs in peace since cyberspace is a constantly restructured domain constructed by manmade efforts to influence the electromagnetic spectrum. Therefore, it is reasonable to presume that shaping and deterring efforts in cyberspace through offensive, defensive, and exploitation efforts, which are categorized traditionally as phase 1 operations for traditional war-fighting domains, will occur in phase 0. This is also where cyber capabilities can have strategic impacts by shaping these phases through "influence operations" in a manner in which cyber power has not previously been used.⁸⁴ If this observation is true, then it is incumbent on policy makers and military forces alike to use national treasures to prepare now for cyber warfare in future conflicts and war. This preparation comes with organizing, training, and equipping a force

to conduct independent or supporting operations while defining what roles other war-fighting domains might play in supporting cyber operations. This is not the first time the United States has been at a decision point regarding building support for a new war-fighting capability.

Unlike the interwar years when the United States appropriated “no investment to original research and development” of aircraft, today’s national and defense appropriations are directly focused on enhancing cyberspace operations.⁸⁵ Now is the time to define the centers of gravity of potential nation-state adversaries and exploit the vulnerabilities to a cost/benefit level acceptable to military commanders and politicians, while developing state-of-the-art offensive cyber weapons and using them when stated policy regarding acceptable cyber behavior is violated.⁸⁶

How to organize, train, and equip cyber forces is crystal clear when military commanders know the defined objectives. Knowing that offensive forces are the primary objective, followed by defensive and exploitation forces, allows commanders to establish priorities for sizing and organizing forces for each needed capability. These priorities also shape weapon system procurement by focusing on offensive tool research, development, creation, and testing of capabilities to achieve desired objectives, followed by tool development for defense and exploitation. Finally, equipping the force to meet its stated objectives is the product of following the defined strategy.

Defining what is needed to equip a force capable of achieving defined objectives determines what training is needed. To put it in simple terms, if new technologies are needed to support offensive operations and those tools require internal development for security or secrecy reasons, then software engineers may be deemed critical to mission success. However, if remote “gap jumping” technology is needed, with Airmen skilled in creating the mobile cyberspace environment—known as cyber extension to some—then training is required to meet those specific needs.⁸⁷ When mission needs are driven by defined roles, then focused efforts on recruiting, training, and equipping the right cyber force become less arbitrary and more deliberate. This leads to the third byproduct of defined targets for Air Force cyber effects: organizing the force.

The Air Force does not own cyberspace, not even the cyberspace for its six defined roles. Whether the Air Force pursues a “closed” network for mission critical roles or pursues functional capability in the “open” network, collaboration with other military services, federal agencies, and the civilian/commercial cyberspace community is necessary. However, given the interconnectedness of cyber operations throughout practically all critical national security interests, does it make more sense to create a consolidated national cyber force where

military, federal, and civilian/commercial industry entities operate under one authority? This is not intended to mandate oversight of cyberspace by the government; governance of rules and compliance mandates would only apply to areas of cyberspace that directly relate to national security.

A quick look at another nation-state might highlight efforts that create more cyberspace efficacy than current US efforts. This observation is driven by the growing number of legislative proposals to increase cybersecurity within the United States that undoubtedly go unheeded for various reasons. First, most commercial businesses and individuals throughout society are not inclined to spend their money to close cybersecurity vulnerabilities that have not affected them. They might believe that the government would pay to fix these vulnerabilities if they wanted them fixed. Second, there might be a belief that current policy and practices regarding cybersecurity are outdated. If the government were to hold the creators and distributors of software accountable for errors in programming code—which is where many known cybersecurity vulnerabilities proliferate—then those manufacturers should be required to “push” software updates to all users free of charge. This would eliminate the individual and corporate expenses of antivirus software, and it would drive better software development before a product release. It would also put ownership of the vulnerability resolution where it belongs, with its creator.

A simple analogy can be seen in the auto industry. When a safety fault is found in a vehicle, the manufacturer is responsible for notifying owners as well as paying for the repair. There is no reason this process could not work in cyberspace. If the vulnerabilities are truly a security threat, then software manufacturers should be responsible for a resolution without relying on the end user. Unlike the car manufacturing scenario, an automated software patch could be pushed globally; the next time the system interacts with the Internet, it receives the fix automatically.

Australian Case Study

Looking at Australia’s activities provides a potential organizational structure that consolidates a nation’s interests regarding cyberspace operations and its desired security regarding those interests. Taking this approach affirms cyberspace as an independent capability requiring an independent force to address its highly technical needs and also eliminates redundancy that inevitably occurs when various forces and organizations develop the same training and equipping needs. It also removes redundancy in additional overhead in running various cyber forces throughout diverse military forces and civilian agencies.

Australia's 2013 *National Security Strategy* identifies tasks assigned to the Australian government, declaring that "our national security is the most basic expression of our sovereignty . . . and national security is the most fundamental task of government."⁸⁸ Of three specific tasks the Australian government is dedicated to over the next five years, "identify[ing] area[s] for increased effort in cybersecurity" is the second task.⁸⁹ To achieve this monumental task, Prime Minister Julia Gillard not only established an office of the cyber policy coordinator to provide leadership and coordination on important cyber issues but also envisioned a new Australian Cyber Security Centre. The center is intended to be "a world-class facility combining existing cybersecurity capabilities across the Attorney-General's Department, Defense, ASIO [the Australian Security Intelligence Organisation], the Australian Federal Police, and the Australian Crime Commission in a single location."⁹⁰

Consolidating efforts, as Australia intends, not only enables a more agile response to government or industry cyber crime and cybersecurity but also creates a hub for greater collaboration among private-sector industry, state and territory governments, and international partners to combat the full breadth of cyber threats.⁹¹ In other words, Australia recognizes cyber threats as a national issue and is combining all required private, public, and government sectors under one organization to create efficacy in addressing cyberspace challenges.

In *Airpower for Strategic Effect*, Colin Gray supports an independent service position, advocating that "an organization dedicated to cyber power is likely to advance understanding and capability of cyber forces."⁹² If the United States were to take this approach, would it resolve known constraints in conducting offensive, defensive, or exploitation efforts in cyberspace by bringing various national agencies under the purview of one responsible agent? Would this structure create a national cyber force that has the legitimacy to operate on the nation's behalf and the authority and ability to quickly respond to perceived threats? Would a quick and consistent response increase the US cyber force's credibility across the globe and thus act as a deterrent?

All of these are questions for discussion and further analysis. Even if the United States does not pursue a consolidated Department of Cyber at this time, it is worth watching other nations that travel this path and conduct not only cost-benefit analysis of such a venture but also monitor cyber threats and vulnerabilities within those nations to determine if the threat trends rise or fall.⁹³ Of course, this passive measure of watching other nations create a required cyber-force structure to address national security vulnerabilities resembles watching other nations develop separate air services during the inter-war period.⁹⁴ Is there a lesson to be learned from being passive during early

airpower development? More directly, is there a lesson to be learned from the early pursuits of airpower, in that to truly exploit airpower, a nation requires strategic thinkers for the domain independent of constraints to other warfare domains? Billy Mitchell highlighted this pursuit regarding airpower when he said, “the time has come when aviation must be developed for aviation’s sake and not as an auxiliary to other existing branches.”⁹⁵

With this in mind, future researchers should examine the question of whether or not cyber power requires an independent arm to project national power led by those who understand and can develop its full potentials in, through, and from the cyberspace domain. This pursuit will not diminish a requirement for the nation’s other military forces to employ cyber-power capabilities to advance effectiveness and efficiency within each warfare domain.

Propositions

Developing a cyber-power targeting theory draws upon the same lesson as Clausewitz did regarding the violence of war as another means for political intercourse. Cyber war is a continuation of this tradition. Therefore, it is important to show how US cyber-war preparation is aided by connecting the six defined Air Force cyber-targeting roles to the three ascribed cyber-warfare roles—offense, defense, and exploitation—to the phases of war in JP 3-0, while correlating applicable principles of war in each phase. The intent is not to create a “strategic bombing theory” such as ACTS developed and US forces ascribed to in World War II. It is intended to initiate a dialogue and to suggest potential testing parameters that determine what works, what does not, and if other principles of war are required to effectively conduct a cyber war. These efforts might be described as *Propositions for Cyber-Power Targeting*.

Proposition 1: *In cyber war, offensive cyber power is the dominant form of cyber warfare.* Offensive cyber activities ensure superiority in cyberspace while aiding the same in the air and space domains of Air Force operations. By controlling a determined spectrum of cyberspace and preventing the adversary from maneuvering in that cyberspace, a friendly force advantage is created. As with any warfare domain, offensive action can be decisive, surprise can create an advantage, and the freedom to maneuver at a pace quicker than an opponent can be desirable. These principles apply to cyber just as they do to air, land, or sea battle.

Proposition 2: *Offensive cyber actions also contribute to rapid global strike due to the inherent speed at which cyber operations are conducted.* The effectiveness of these offensive operations is dependent on accurate intelligence

and the shaping of cyberspace before and during operations. Additionally, offensive cyber can affect the command and control of an adversary and impact its nuclear deterrence capability. The effects described may be achieved indirectly by targeting supervisory control and data acquisition vulnerabilities and software vulnerabilities or directly by active hacking into systems for real-time control, activating logic bombs to enable desired effects, or using social engineering to make an adversary believe friendly forces are conducting authorized and legitimate activities.

Proposition 3: *The offensive, mass, surprise, maneuver, unity of effort, legitimacy, and proportionality principles of war are most prevalent in offensive cyber operations.* Although all principles of war defined in joint publication or Air Force doctrine will apply to offensive cyber operations at some point, the principles most prevalent are the following: offensive, mass, surprise, maneuver, unity of effort, legitimacy, and proportionality, which replaces the restraint principle defined by the Air Force.

Proposition 4: *Offensive cyber operations impact all phases of war but may be most effective in earlier phases for shaping and initial action.* As for which phases of war offensive actions can and should occur, I argue that it impacts all of them. However, the focus of offensive cyber action should be in phase-0 and phase-1 in order to shape the environment by conducting operations to deter an adversary from escalating to war. Then, if war starts, full scale offensive cyber operations should occur in phase-2 and phase-3—not only to gain and maintain control of cyberspace but also to initiate actions that inhibit an adversary's air, land, and sea operations where possible through cyberspace. Finally, offensive cyber actions can assist phase-4 stabilization efforts by countering adversary actions that oppose friendly political objectives. These may include information operation campaigns that support legitimate actions of those suing for peace while inhibiting access in cyberspace for those who oppose peaceful negotiations.

Proposition 5: *Defensive cyber operations are futile if not focused and will not conclude a war. Nations should not attempt to defend all of cyberspace.* Defensive cyber operations primarily support phases 0, 1, 2, and 4 military operations, although there is a standing requirement for ongoing defensive cyber measures both in peacetime and in war. There will always be a need for passive and active defensive measures to protect US national security interests supported by, or potentially affected through, cyberspace. However, defensive cyber operations are not decisive in nature and will not resolve conflicts in cyberspace nor conclude war of any form.

Proposition 6: *Defensive cyber operations are most relevant when automated response actions occur based on active sensors.* Relative to the defined

Air Force cyber-target roles, defensive cyber operations primarily support air, space, and cyberspace superiority measures through passive and active cyberspace defense mechanisms. Using sensors to detect and report network system anomalies would be one such measure. The overused pursuit of “software patching” on open government systems would be another.⁹⁶ The software patching fallacy is that its actions are mostly reactive to identified vulnerabilities. For this reason, automated responses must be developed to protect cyberspace compared to national security interests. If human interaction is required to reduce the vulnerability, the time required for any such action will be an inhibitor due to the speed at which actions occur in cyberspace. Whatever useful method for cyberspace defense is employed, these roles must also support offensive objectives while protecting critical national security targets from adversarial affects.

Proposition 7: *Defensive cyber forces can rapidly transition to offensive roles, thus providing a reserve cyber force for commanders.* These defensive tactics cannot achieve political objectives in and of themselves. However, if needed, the defense forces can rapidly transition to offensive forces to provide either a counterattack against an adversary’s offensive attack or a reserve force if additional offensive forces are needed to exploit a cyberspace gap. Defensive cyber operations can also protect intelligence, surveillance, and reconnaissance; command and control; and nuclear deterrence functions. Operations in these realms are relegated to protecting the information relied upon within these mission sets, while potentially conducting disinformation campaigns through deception techniques such as “honeypots.”⁹⁷ By conducting these operations, cyber forces can learn adversary techniques that assist further development of offensive cyber forces and operational techniques.

Proposition 8: *Economy of force, simplicity, security, and perseverance are the primary principles of war used in conducting defensive cyber operations.* Because cyberspace is a constantly changing domain, and the adversary is capable of thinking and adjusting to counter new techniques and technology, attempting to defend the entire cyberspace domain is fruitless. Some might argue that China is competing with the United States by creating havoc in cyberspace, thus pushing the United States to counter threats by all necessary means short of kinetic warfare. If the United States intends to fight that battle, it could potentially be more expensive in the long run than the Cold War with the Soviet Union was.⁹⁸ As Cold War military capabilities were developed and established, maintenance and readiness of the force were the only recurring costs. Although the costs of cyber technology are extremely cheap to create and maintain relative to a nuclear arsenal, the damage caused by one offensive cyber attack can potentially be extreme.⁹⁹ Supporting such a claim today is

challenging, as many organizations that have suffered a cyber attack may not report it. Therefore, the actual cost of damage or the monetary equivalent in lost information or assets is incomputable.

Proposition 9: *Closed networks are the best protection from an adversary's cyber operations.* Employing the right-sized force to provide cybersecurity of true national security interests will limit what cyber forces must protect. This keeps the defensive measures focused and simple. It does not mean cyber-defense techniques are simple versus complex; defense in depth is an absolute must. Persevering through varying cyber attacks ensures the survivability of required national capabilities so they are available when called to action by policy makers. Of course, one of the best defenses in the cyberspace battle is to separate critical networks from the less critical. In other words, employ a closed network for critical capabilities versus an open network.

The battle for open versus closed networks has already begun. Could it be that authoritarian governments have recognized how vulnerable all war-fighting domains are, given the pervasiveness of cyberspace, and are taking the first steps to minimize risks? In an attempt to institute governmental controls upon the open Internet, 89 countries voted in favor of allowing each nation the authority to close off access to the Internet in their countries.¹⁰⁰ Although 55 of the 193 nations voted against the International Telecommunications Union proposal, the treaty is set to take effect in 2015 without binding its rules to those opposing nations. However, even though nations that opposed the treaty are not bound to it, they will be affected by its actions. The global network will be split into two camps—open networks and closed.¹⁰¹ This does not change the required offensive, defensive, and exploitation actions in cyberspace but may require a change in the tools and techniques to successfully accomplish them.

Proposition 10: *Exploitation in cyberspace is intelligence gathering and will always endure in cyberspace operations and continue throughout all phases of war.* Exploitation is the final capability to connect to defined roles, military phases, and principles of war. Defined policies will shape Air Force exploitations in cyberspace. Once decision makers establish policy surrounding cyberspace operations and define what constitutes acts of aggression or acts of war, those conducting acts of exploitation in cyberspace may be more constrained than they are today. Regardless, it is proposed that exploitation actions do and will continue to occur in five of the six defined Air Force roles: air, space, and cyberspace superiority; intelligence, surveillance, and reconnaissance; global strike; command and control; and nuclear deterrence.

These exploitation actions are against friendly forces to test system resiliency in the form of red teams and against potential or known adversaries in the form

of intelligence gathering.¹⁰² Exploitation will create the greatest effects during phase-0, 1, and 5 of military operations; however, just as offensive and defensive efforts will cross the full spectrum of military operations, so too will exploitation. Using cyberspace to create vulnerabilities found during exploitation is accomplished with greater autonomy when uncontested. For that reason, the three phases of military operation recognized may presumably be the least contested because they occur before active war begins or immediately at the conclusion of warfare.

To gain the most effort from cyberspace exploits, several necessary principles of war—unity of command, exploitation of defined targeting objects, economy of force, and perseverance—must be used. Given the efforts of exploitation, collaboration is required across the varying US civilian and governmental agencies. Without effective collaboration, there will inevitably be cyberspace fratricide because exploitations may overlap a target when multiple agencies target the same objective. Cyberspace fratricide could also occur when multiple cyber exploit tools are used on the same objective, ultimately causing unneeded waste of valuable capabilities. Of the many challenges to generate effective cyberspace exploitation operations, researching and developing effective tools may be the most relentless requirements. Unlike other domains where technology aids in developing long term fifth-generation stealth fighters, new stealth submarines, or high-speed armored personnel carriers, the technology for cyber exploits, as well as some offensive tools, can have a relatively short shelf life and may be good for only one use. These are facts driven by the dynamic nature of cyberspace and its constantly changing character.

Despite the challenges to exploitation efforts and the fact that it exists to aid both offensive and defensive cyber operations and all other war-fighting domains, its value cannot be understated. In future wars where it may not be nation-state versus nation-state, the more information regarding cyberspace vulnerabilities the United States possesses and the greater its development of exploits that will have known effects, the more prepared US forces will be for the next war. Preparing for war requires having known capabilities to present to combatant commanders during planning and execution in order to bring about a decisive victory. If a commander employs cyber capabilities that create a loss of confidence in the adversary's command and control before battle begins, one can only imagine the true fog and friction that will occur if that adversary presses for war—compound that confusion with other factors that will result in an all-out cyber offensive upon determined centers of gravity, while synchronized with other war-fighting capabilities across all domains.

Overwhelming the enemy is clearly the principle objective for rapid capitulation in war.

Anticipation

Figuring out how and when to employ the offensive, defensive, and exploitation capabilities in cyberspace is a constant challenge for military forces today. This is especially true in an environment of unresolved legal concerns surrounding actions in cyberspace, undefined policy regarding acceptable and unacceptable cyberspace behaviors, and the gray area surrounding potential reactions to cyber threats given the challenges of attribution. However, these concerns do not justify inaction in planning, developing, and validating cyber capabilities. The US *National Security Strategy* calls for the protection of American citizen's security, prosperity, and values and the international order. I argue that cyberspace is eroding each of these stated interests within US borders and internationally every day. The rules regarding the theft of intellectual property and US secrets—compromising the United States' known technical advantages—are undefined in international law and not yet classified as illegal activity in cyberspace—at least not for all nations.¹⁰³ If left unchanged, nations will continue to lose trust both domestically and internationally as actors within cyberspace conduct acts of crime, terrorism, and espionage. How long can the United States afford not to step out and take a lead role in establishing standards and acceptable behaviors throughout cyberspace?

Despite these challenges, many steps are being taken to counter known threats and prepare for future warfare that includes cyber war. Lawyers are pouring through laws of armed conflict and international and domestic laws at an unprecedented rate to determine what, if any, changes need to be made.¹⁰⁴ There is little doubt some laws will change, presumably in the area of identifying and responding to initial cyber threats. It should not matter what virtual force, civilian or military, respond to stop an initial cyber threat, as long as the threat is mitigated. To achieve these results, at least domestically, the delineation between Guard and active duty forces or some other national, state, or local law enforcement agency tasked to respond with a physical presence must become seamless in order to respond to cyber threats.¹⁰⁵

Technologies continue to improve and will eventually resolve the perceived attribution challenge within cyberspace. This challenge is much less than it was just a couple of years ago because forensic testing is getting better both in technology and by virtue of doing more of it. As with anything, the more

something is done, the more practitioners tend to improve at doing it. This leads to the continual advancement of education and training in all cyber areas. As threats like denial of service emerge as major risks to operational success, education and training will increase along with advances in the technology to counter these threats. The intent should not be to eliminate these types of threats; however, controlling and containing them so they do not prevent mission success are absolutely realistic and attainable objectives.

As US society continues to see cyberspace vulnerabilities and the ripple effect in damage that it can cause, mostly in replacement costs of technical capabilities and loss of consumer confidence, pursuit of government involvement to control cyberspace threats will grow. In the commercial industry, for activities that do not directly threaten the society as a whole or its national security interests, those challenges will provide capitalistic opportunities for problem resolution. Government oversight will occur for cyberspace threats that challenge sovereignty, a society's cultural beliefs, and its security. When this call for government intervention occurs, the loss of anonymity, which some pundits argue as the nemesis to greater cybersecurity, will become a thing of the past. This same sort of evolution has occurred since the beginning of time and will continue to occur as societies progress no matter what new technologies evolve or how many freedoms societies pursue.¹⁰⁶ As long as human nature remains unchanged, the principle concern of survival will mandate that there will be a need to create order in the anarchic world in which man lives.¹⁰⁷

Testing

If the object of science is knowledge and the object of art is creative ability, the proposed theory regarding offensive, defensive, and exploitation of cyberspace is art.¹⁰⁸ By defining specific cyber targets to help shape, organize, train, and equip endeavors for Air Force cyber forces and presumably all US military forces, as well as national objectives involving cyberspace, the appearance of a scientific way for cyber war seems prevalent. However, this is a fallacy. Without experience, facts, or tested theories, a normal science of cyber war does not exist, at least not until it has been tested.¹⁰⁹ This is the very reason I believe testing is required for this theory's development. Without testing or experience to rely upon, is an untested theory just a hypothesis?¹¹⁰

Efforts to test cyber capabilities are well under way, as are efforts to include cyberspace operations into existing Air Force functions. Air Combat Command is currently updating a targeting roadmap that intends to incorporate

cyber targets into the current Air Force targeting cycle.¹¹¹ This includes building targeting folders, collecting intelligence, and at least having applicable discussions of where cyber fits into the current Air Force targeting doctrine. But does this process allow cyber to conduct its full spectrum capabilities? Are the targeting objectives based on effects enabled by cyber power and offensive tools available to a combatant commander, or is cyber relegated to a support role with airpower capabilities at the center of offensive planning efforts? These questions are beyond this treatise but are worth future debate. Just as discussions about airpower and its relevance as an independent fighting force were worth having in the early 1900s, so too should cyber power's unbounded capabilities be explored to determine its role as a military power and its ability to achieve political objectives. Regardless of the outcome, by including cyber discussions and potentially testing capabilities, the proposed cyber-power targeting theory can move toward a true theory as continual experience is gained.

Other efforts to test cyber-power abilities expand continually in joint cyber exercises.¹¹² Over the past few years, the cyber injects have gone from white-card notional applications of cyber power to true operational testing of cyber capabilities. The lessons learned from second- and third-order cyber effects in the exercise scenarios certainly aid continual improvements. Expansion in military cyber ranges enables integrated training and education not only within the Air Force but also with sister services and civilian agencies.¹¹³ These low-cost resources pay huge benefits by bringing disparate cyber operators to a common understanding of the contested cyberspace environment. This also allows for the real-time sharing of cyber tools and techniques that improve cybersecurity practices, while testing new capabilities off the "live network."¹¹⁴

Testing this theory requires more than just validating technological capabilities of cyberspace tools. Cyberspace relies on human capital to create affects in the cyber domain. One could argue this is true for all domains, but it is especially the case for cyberspace. Without human capital, the cyberspace domain has no need to exist or function, since its purpose is to serve societal needs. This is not true for the other domains. Land, air, sea, and space would all continue to exist without human intervention. Together these global commons constitute the connective tissue of the international system affecting various aspects of societies.¹¹⁵

It is important to continually test the ongoing education, training, and experiences of human development regarding cyber forces given this reliance of the cyberspace domain on humans. If US military forces are going to dominate in cyberspace, capital investments in higher education, state-of-the-art training centers, and operational experience are critical to success. Once

this occurs, the cultural development needed for consistent cyber activities can be facilitated.¹¹⁶ However, US forces must be cautious in the pursuit to make the perfect cyber operator.

Despite theories such as cybernetics and chaoplexity espoused by Antoine Bousquet, which pursue both the human drive for complete predictability and the desire for control in warfare, those goals should not be the human pursuit in regards to cyber war.¹¹⁷ Historical examples continually remind us that the pursuit of complete predictability is unattainable; however, there are actions that can reduce some fog and friction in war. Efforts such as incorporating cyber warriors into existing weapons instructor courses are a great first step.¹¹⁸ This program provides an opportunity for other combat Air Force platforms to understand what cyber power can do and exposes cyber operators to other combat platforms. The results are a greater understanding of existing capabilities and potentially better integration of combat efforts.

Another positive movement by the Air Force is professing the need to stand up a Cyber Air Corps Tactical School to expand strategic thinking regarding cyber capabilities while evolving doctrine on the subject.¹¹⁹ Efforts like this develop the human aspect by discussing the art of the possible relative to cyber-power projection, while creating an environment to analyze academic rigor and determine required adjustments to continually develop the force and the cyber-power strategies to be used by the force. Although these early discussions may not provide the best possible results in the first cyber war, they will provide a foundation for future discussions as knowledge is gained, feedback is received, and new challenges arise.

The final piece of testing discussed in this treatise revolves around obtaining lessons learned in operations and applicable metrics for measuring intended cyber results. This may be one of the most challenging objectives—to develop meaningful battle-damage assessment of cyber-power effects. Although cyber power has the ability to be extremely precise in its targeted effects, it also has the potential to create massive unintended second- and third-order effects if fail-safes are not embedded correctly. Stuxnet may be a great case study to make this point. It has been argued that Stuxnet was created with a specific target in mind. However, when the Stuxnet exploit crossed over from a closed network to an open one, it had the potential to create unintended havoc. Gathering feedback from events such as Stuxnet can aid offensive, defensive, and exploitation operatives to develop effective tools and preventative mechanisms as applicable. This will help minimize unintended collateral damage while operating within tolerable risk parameters. The challenge is gauging how quickly these successes or failures are measured so the

information is timely and useful. Once again, this is a question for future study but one of relevant importance.

Summary

Early skeptics of airpower stated airpower can “hold nothing.”¹²⁰ Recognizing that fact did not constrain the thinking of airpower advocates who sought to expand military capabilities within the newest warfare domain of the time. The same skeptics stated airpower could not hold its ground and fight. This proved to be incorrect in the sense that if a nation was willing, it could expend the necessary resources to establish and hold air supremacy. The same can be said in regard to cyber power today.

Conducting operations in, through, and from cyberspace requires unbounded evaluation of the art of possible while recognizing the limitations inherent to the nature of cyber operations. Cyber operations will never hold the physical terrain to which ground commanders refer. I suggest that holding ground is not a requirement of cyber operations nor should it be—at least not until the ground force is robotic, at which point cyber forces can hold the ground. As long as US national security is protected from harmful cyber attacks and effective US cyber operations are enabled to meet political objectives, then the efficacy desired is achieved.

Cyberspace is changing most rapidly among war-fighting domains, because it is the only man-made domain where warfare can occur. Recognizing this fact, despite the minimal expense of operating in cyberspace, highlights the fact that permanently holding the cyberspace ground is unattainable. However, controlling a portion of the cyberspace domain, while conducting required operations, is quite probable. Protecting US vital interests from cyberspace threats requires the Air Force and other services to not only employ cyber power within this war-fighting domain but also to dominate portions of it to ensure operational success is achieved across all war-fighting domains.

Just as nations build airplanes to dominate air, ships to dominate sea, and tanks to dominate land, so too must nations build cyber technology and develop cyber warriors to dominate cyberspace. If the cyber-power targeting theory espoused aids in continual doctrine development and strategic thinking regarding the possibilities of cyber power and is considered during OT&E decisions for cyber forces in the USAF and potentially national level, then the intent of this treatise is achieved.

Given the lack of cyber-war and cyber-warfare experience, limited definitions regarding what constitutes cyber war, and minimal cyber-war doctrine

publishing, maybe the best this thesis can suggest is a hypothetical theory for strategic cyber power. Based on my understanding of Clausewitz, familiarity with a theory requires analytical investigation with the subject and applied experience—relative to military history in this case—to gain thorough familiarity with it.¹²¹ Theory then becomes a guide to anyone who wants to learn about war in books, preventing warriors from starting warfare studies afresh each time war occurs.¹²² Either way, the fact that cyber power is being discussed and theories of cyber war are evolving, gives me confidence that the US military will continue to develop cyber-warfare capabilities and enable independent and integrated cyberspace operations in order to win the nation's future wars.

Notes

1. Clausewitz, *On War*, 141.
2. Winton, "An Imperfect Jewel," 853–77.
3. Clausewitz, *On War*, 250.
4. *Ibid.*, 256.
5. For an understanding of the combined arms concept, see MCDP 1, *Warfighting*, 55.
6. Olsen, *John Warden and the Renaissance of American Air Power*, 108.
7. Gray, "Airpower Advantage in Future Warfare," 8.
8. *Ibid.*
9. JP 1-02, *Department of Defense Dictionary*, 317.
10. MCDP 1, *Warfighting*, 71.
11. When the United States entered the war in 1942, American Air Force leaders believed they could overcome the obstacles British air forces encountered during the combined bomber offensive. Initially Americans were against using aerial weapons to bomb civilians and civilian targets. A flawed doctrine led to the belief that bombers could defend themselves in massed formations. Further details are in Tanaka and Young, *Bombing Civilians*, 36–37.
12. Gray, "Airpower Advantage in Future Warfare," vii.
13. *Ibid.*
14. Clausewitz, *On War*, 138.
15. Lonsdale, *Nature of War*, 22.
16. *Ibid.*
17. Douhet captured the idea of crushing the material and moral resistance of the enemy without regard to military or civilian losses in the first of his 11 principles of air power. Douhet, *Command of the Air*, 128–29.
18. Pape, *Bombing to Win*, 331.
19. *Ibid.*
20. My use of *absolute* or *total* versus *limited* war is based on an understanding of Clausewitz in which total war places "no logical limit to the application of force." In other words, an opposing force will use the "total means at his disposal" to overcome an enemy. I call this *theoretical warfare* and suggest this is the warfare military commanders prefer, as there are no limits on capabilities and actions in warfare that would theoretically aid in rapid capitulation by an adversary. However, as Clausewitz develops his theory of war, he reminds readers of the difference in desired war

and reality, or what he calls war in practice, not what its ideal nature ought to be. Future wars, according to Clausewitz, “will be severely restricted.” Limited aims of warfare will dictate limited offensive and defensive war. These limitations are the product of the nature of political aim, the scale of demands put forward by both sides, and the total political situation of one’s own side. Wars conducted by the United States since World War II where unconditional surrender was required appear to favor limited verse absolute warfare. Clausewitz, *On War*, 593–602.

21. MCDP 1, *Warfighting*, 2–3.
22. AFDD 1, *Air Force Basic Doctrine*.
23. Ibid.
24. Kainikara and RAAF Air Power Development Centre, *Principles of War and Airpower*, 6.
25. See the propositions General Williams proposes regarding command and control of cyber force operations by the combatant commander, just as all other warfare domains are currently controlled. He is also an advocate of creating a JFACC so there is one commander responsible for cyber operations within the combat area of responsibility. Williams, “Ten Propositions Regarding Cyberspace Operations.”
26. Libicki, “Military Cyberpower,” in Kramer, Starr, and Wentz, *Cyberpower and National Security*, 47.
27. Vautrinot, “Sharing the Cyber Journey,” 72.
28. An alternative definition, although I do not believe it is a clear definition, is that cyberspace is considered a fifth dimension where people can exist through alternate persona in virtual reality. Reveron, *Cyberspace and National Security*, 5.
29. Stuart H. Starr, “Toward a Preliminary Theory of Cyberpower,” in Kramer, Starr, and Wentz, *Cyberpower and National Security*, 47–48.
30. See principle five of General Williams’s 10 principles for details regarding the man-made domain and how it can be influenced by man. Williams, “Ten Propositions Regarding Cyberspace Operations,” 14.
31. *Webster’s Student Dictionary*, s.v. “cyberspace,” 211.
32. For information on Stuxnet and its effects, see Brenner, *America the Vulnerable*, 102; and Reveron, *Cyberspace and National Security*, 11.
33. Gregory Rattray, “An Environmental Approach to Understanding Cyberpower,” in Kramer, Starr, and Wentz, *Cyberpower and National Security*, 274.
34. Starr, “Toward a Preliminary Theory of Cyberpower,” 48.
35. Clausewitz, *On War*, 141.
36. Winton, “An Imperfect Jewel,” 853–77.
37. “The political object is the goal, war is the means of reaching it, and means can never be considered in isolation from their purpose.” Clausewitz, *On War*, 87.
38. Ibid., 75–87.
39. Finney, *History of the Air Corps Tactical School*, 3.
40. Winton, “An Imperfect Jewel,” 856.
41. Clausewitz defined war as “an act of force, and there is no logical limit to the application of that force.” This definition succinctly defines war for the perspective of this study. Clausewitz, *On War*, 77.
42. Winton, “An Imperfect Jewel,” 856.
43. Recent articles that speculate where the cyber attacks came from can be found in online articles. Nicole Perlroth, “Washington Post Joins List of News Media Hacked by the Chinese,” *New York Times*, 1 February 2013, http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0.

HYPOTHESIZING A CYBER-POWER TARGETING THEORY

44. Sheep do not like the sheepdogs because they look like a wolf with fangs and the capacity for violence. The difference, though, is that the sheepdog must not, cannot, and will not ever harm the sheep. Any sheepdog who intentionally harms the lowliest little lamb will be punished and removed. The world cannot work any other way, at least not in a representative democracy or a republic such as ours. This analogy provided by retired colonel Grossman mirrors the general public (the sheep), terrorists or aggressive nation-states that seek war with the United States (wolves), and US military forces, including any public protective service like local and state police, the FBI, and others (sheepdogs). Grossman and Christensen, *On Combat*, 182–83.

45. Lynn, “Pentagon’s Cyberstrategy.”

46. DOD, Department of Defense Cyberspace Policy Report, 2.

47. For a guide to improving existing infrastructure components or building new ones, see Amoroso, *Cyber Attacks*, 9–11.

48. Clarke and Knake, *Cyber War*, xiii.

49. *Ibid.*, 6.

50. Charter of the United Nations, chap. 1, art. 2, sec. 4.

51. The ICJ in *US vs. Nicaragua* discussed the right of self-defense: “The general rule prohibiting force established in customary law allows for certain exceptions. The exception of the right of individual or collective self-defense is also, in the view of States, established in customary law, as is apparent for example from the terms of Article 51 of the UN Charter, which refers to an ‘inherent right’; and from the declaration in resolution 2625 (XXV).” Whether self-defense is individual or collective, it can be exercised only in response to an “armed attack.” In the view of the court, this is to be understood as meaning not merely action by regular armed forces across an international border but also the sending by a state of armed bands onto the territory of another state, if such an operation, because of its scale and effects, would have been classified as an armed attack had it been carried out by regular armed forces. However, the court stated that “states do not have a right of ‘collective’ armed response to acts which do not constitute an ‘armed attack.’” *Case Concerning the Military and Paramilitary Activities*.

52. To read specifics on United Nations and Security Council actions, see the Charter of the United Nations.

53. *Ibid.*

54. See information regarding the founding of the United Nations, <http://www.un.org/en/documents/charter/intro.shtml>.

55. *Jus ad bellum* discusses actions leading up to war to aid in determining if actions before war made the act of going to war *just*. *Jus in bello* evaluates actions in war to determine if war was conducted in a *just* way. For additional details on both *jus ad bellum* and *jus in bello*, see Walzer, *Just and Unjust Wars*.

56. For an exceptionally good discourse regarding cyber attacks and the challenges facing the United States and the international community alike surrounding this issue, see Waxman, “Cyber Attacks and the Use of Force,” 421–59. Also see the definition of *cyber attack* in Schmitt, *Tallinn Manual*, 106.

57. JP 3-12, *Cyberspace Operations*, III-3.

58. See the National Security Archives for existing and past *National Security Strategies*, <http://nssarchive.us/>.

59. For specific details regarding US national security, see *National Security Strategy*, 17.

60. Welsh, “A Vision for the United States Air Force.”

61. US Air Force, “2013 Air Force Mission Statement.”

62. US House, *Department of the Air Force Presentation*.

63. Before this list is final, the Air Force should clearly define what air, space, and cyberspace superiority is. Once defined, a determination should be made as to whether or not each objective is achievable or desired. Specifically, if cyberspace superiority is having the ability to operate in a contested cyberspace environment, that may be achievable. If cyberspace superiority is controlling the entire cyberspace, that may be an unattainable objective.

64. Gen Bradford Shwedo, director of intelligence, Headquarters Air Combat Command, interview with the author, 2 November 2012.

65. Most of Col John Boyd's information surrounding his OODA loop exists in presentation format and not a published book. For a synthesis of his works see Osinga, *Science, Strategy and War*.

66. Clausewitz, *On War*, 131.

67. *Ibid.*, 484.

68. The use of "active adversarial capabilities" alludes to a similar meaning Secretary of Defense William Cohen noted in his memorandum to US military leaders regarding a new DOD Space Policy in 1999. The point is that any direct action against US assets will be considered an act of aggression. Secretary Cohen said that "purposeful interference with US space systems will be viewed as an infringement on our sovereign rights." Donnelly, "Cohen," 2.

69. Libicki, *Cyberdeterrence and Cyberwar*, 33.

70. Schmitt and Shanker, *Counterstrike*, 135.

71. Nations around the world are expanding their cyber forces and growing capabilities, despite shrinking defense budgets. The United States is doing the same. When countries like Israel threaten preemptive strikes against an adversary that include cyber attacks on command-and-control networks and communications and infrastructure to degrade military capabilities, it is clear cyber-power projection will occur at the earliest stages of warfare. "Israel Builds Up Its Cyberwar Corps," *United Press International*, 2 November 2012, http://www.upi.com/Business_News/Security/Industry/2012/11/02/Israel-builds-up-its-cyberwar-corps/UPI-52421351881449.

72. Brenner, *Cyberthreats*, 81.

73. A zero-day cyber attack is an unknown exploit that proliferates throughout cyberspace to which no known defenses initially exist. The Conflicker worm is an example of a zero-day exploit which, to some observers, was known as a "digital blitzkrieg." Bowden, *Worm*, 23.

74. Malware is available on the open market that offers a "service level agreement and replacement warranty if the purchased malware is detected by any anti-virus software within nine months." This affirms that those who employ malware do not perceive a threat from anti-virus software for at least nine months. Suffolk, "Cyber Security Perspectives."

75. Additional inferences regarding network detections taking an extended period can be seen in comments by Gen Keith Alexander, commander of USCYBERCOM and director of the National Security Agency. He stated that "when people break into a network, they're often there for six to nine months before we detect them." While in the network, the attackers "own the networks" for that time and have the ability to take whatever they want. Cameron Cox, "NSA Director on Cyberattacks: 'Everybody's' Getting Hit," *ABC News Radio*, 7 November 2012, <http://abcnewsradioonline.com/business-news/tag/hackers>.

76. Logic bombs are a set of instructions that are intentionally designed to execute when a particular condition has been satisfied. These bombs commonly delete or corrupt data, reset passwords, or have other harmful effects. These malicious programs can be introduced through a variety of means, months or even years before they need to be triggered for a specific operation. Bumgarner, "Computers as Weapons of War," 6.

77. Elihu Zimet and Charles Barry, "Military Service Overview," in Kramer, Starr, and Wentz, *Cyberpower and National Security*, 288.

HYPOTHESIZING A CYBER-POWER TARGETING THEORY

78. Ibid.

79. Rid, "Cyber War Will Not Take Place," 6.

80. For an understanding of vulnerabilities surrounding cyberspace and social engineering tactics currently being employed in cyberspace, see Hadnagy and Wilson, *Social Engineering*, 2.

81. "Botnets' Run Wild," *Washington Post*, 24 January 2013, <http://www.news-herald.com/articles/2013/01/24/opinion/nh6474510.txt>.

82. Ibid.

83. Center for Global Development, *Phase Zero*.

84. Col Paul Welch is the current commander of the 688th Information Operations Wing, Lackland AFB, Texas. During a telephone interview, he suggested that traditional Air Force roles of compass call or air drops of leaflets during phase 1 and earlier operations may have to change in order to gain the full effects afforded by cyberspace. He goes on to say that "maneuver through the domain requires constant attention through and to the target. There are four areas we must focus on: target selection is complex, maneuver to the target and having the ability to have a technical affect is required, determine if the effect is what we are looking for, and how can I assess the result?" Welch affirmed that cyber power capabilities must provide "a variety of options to COCOMS," just as all war-fighting domains should, but that cyber capabilities should not be confined and prevented from achieving their full potential. Col Paul Welch, 688 Information Operations Wing commander, interview by the author, 12 December 2012.

85. De Seversky, *Victory through Air Power*, 218.

86. At a time when the US defense budget is shrinking across most major weapon systems, USCYBERCOM and service-specific funding requests for cyber operations were approved and in some cases saw an increase in funding. This is a clear message that cyberspace threats are starting to be recognized as detrimental to national security interests. For specifics on US defense spending surrounding cyberspace, see US House, *2013 National Defense Authorization Act*.

87. The term cyber extension is sometimes used in mobile communications circles like combat communications. Cyber extension refers to the ability to bring cyberspace to a place it currently does not exist through deployable mobile assets that enable connection to cyberspace with mobile satellites, switches, and routers in order to connect to the global information grid.

88. I am indebted to my Australian counterpart in SAASS Class XXII, Squadron Leader Travis Hallen, for bringing this document to my attention. To read the full article detailing Australia's national security strategy, see Julia Gillard, Prime Minister of Australia, "Australia's National Security Beyond the 9/11 Decade," press release, 23 January 2013, <http://www.pm.gov.au/press-office/australias-national-security-beyond-911-decade>.

89. Ibid.

90. Ibid.

91. Ibid.

92. Gray and Lambeth, *Airpower for Strategic Effect*, 300.

93. *Department of Cyber* is my term for what the United States might create by combining public and government forces together to protect national security interests regarding cyber and conduct the full spectrum of cyber operations on behalf of the United States in both domestic and international cyberspace.

94. Following the Second Balkan War, which ended in 1913, many nations recognized the importance of the air weapon and began creating independent air services for national defense. The Royal Flying Corps (April 1912), the Direction de l'Aéronautique Militaire in France (April 1914), and the Corpo Aeronautico Militare of Italy (January 1915) were early independent air services. Kennett, *First Air War*, 20.

95. Mitchell and Ehlers, *Winged Defense*, X.

96. Software patching is a software fix distributed by a manufacturer, such as Microsoft, to close a known vulnerability. Some software vendors will not support customer needs if software patch updates are not applied and up-to-date. This process requires the end user to constantly monitor for software updates and is a reactive process that requires manual intervention by users. A 2004 survey of US electrical operators found “loosely controlled system access and perimeter control, poor patch and configuration management, and poor system security documentation.” Another study found certain systems took an average of 331 days to implement software patch updates. That means vulnerabilities remained for almost an entire year before being corrected. Imagine flying an airplane with a known cracked wing for 331 days. Brenner, *America the Vulnerable*, 98.

97. Honeypot is a computer, usually virtual, without any security safeguards—in other words, designed to be infected by malware. Bowden, *Worm*, 248.

98. The average annual cost to the US military during the Cold War years is estimated at \$298.5 billion. The cost of protecting, maintaining, and repairing damages caused by cyber attacks is unknown today but should be tracked more accurately to truly assess costs of cyberspace to the nation. See Calhoun, *US Military Spending*.

99. According to the Ponemon Institute study, which is based on a sample size of 50 “larger-sized organizations,” the cost of cyber crime has gone from an average \$3.8 million per company to \$5.9 million per company for one year. That represents an increase of 56 percent in one year. Obviously, this example may not correlate directly to cyber threats to national security, but based on the importance of centers of gravity discussed in chapter 4, it is safe to presume that cyber attacks and threats to national security interests are, at a minimum, comparable to these corporations. If damage from cyber attacks continues to increase at a rate of 56 percent per year, defense spending to protect national security interests enabled by cyberspace must keep pace with these threats or succumb to adversarial effects. Ponemon Institute, “Second Annual Cost of Cyber Crime Study.”

100. Gordon Crovitz, “America’s First Big Digital Defeat,” *Wall Street Journal*, 16 December 2012, <http://online.wsj.com/article/SB10001424127887323981504578181533577508260.html>.

101. Although the Internet was designed to be a place for freedom of information interchange without regulation or governance, the creation of closed portions may hinder operations in cyberspace. But in reality, this is nothing new. Companies have used closed systems since the Internet’s creation; the difference is that they have also paid for closed circuits to support the closed systems. This proposal allows for “control over Internet companies, not just telecoms” through its declaration that “all governments should have an equal role and responsibility for international Internet governance.” The fallacy in this thought process is that not all governments equally provide the Internet, and the realists would argue those with the most power should get the biggest voice. Ibid.

102. Red teaming is considered by some to be the “most effective tool we have for testing the security of an information system.” In simple terms, it is an organization established to probe an organization for security vulnerabilities either through hardware or software misconfiguration or established processes for interacting in, through, or from cyberspace. Brenner, *America the Vulnerable*, 222.

103. Part of the challenge in defining international rules surrounds the lack of common terminology for cyber-related activities. Accepting common definitions for terminology such as *cyber crime*, *cyberterrorism*, and *cyber warfare* is one start to developing international standards. Susan

HYPOTHESIZING A CYBER-POWER TARGETING THEORY

Brenner offers a common lexicon to consider. Once the lexicon is agreed upon, then international standards of behavior within cyberspace may begin to evolve. Brenner, *Cyberthreats*, 29–54.

104. For a detailed three-year research project regarding international laws surrounding cyber war, see the work of 20 international law scholars and practitioners. This work lays out 95 rules governing cyber warfare. The rules range from actions before cyber war to conduct in war, as well as international humanitarian law and laws of neutrality. Schmitt, *Tallinn Manual*.

105. Within the domestic realm, US military forces operating under Title 10 authorities are prohibited from conducting military operations without special provision. The 1878 Posse Comitatus Act created a distinction between military and civilian law enforcement within the United States. It is laws such as these that require consideration in order to resolve response actions to cyber threats. Brenner, *Cyberthreats*, 177.

106. Susan Brenner discusses how, by the mid-twentieth century, nation-states monopolized the legitimate use of force to maintain order, both internally and externally. They relied on professional, uniformed, hierarchically organized warriors to resolve external conflicts arising with other nation-states. They also relied on professional, uniformed, and hierarchically organized law enforcement officers to maintain internal order by reacting to the commission of crimes within the territory the nation-state controlled. This is the same premise that should be considered to control cyber crimes as it has and continues to work for other protection of the nation-state and its citizens. *Ibid.*, 23.

107. Kenneth Waltz claims there is no automatic harmony in anarchy. Waltz is referring to the order of the international system and relation between states as he describes the world order as a system of anarchy. He states that with no system of law enforceable among sovereign states, each state will judge its grievances and ambitions according to the dictates of its own reason or desire—conflict sometimes leads to war. Concerns regarding international order of acceptable norms within cyberspace exist in this same system of anarchy that is the international system today. Waltz, *Man, the State, and War*, 160.

108. Clausewitz, *On War*, 149.

109. In discussing normal science, Thomas Kuhn says science is the constellation of facts, theories, and methods collected in texts. It is these accepted scientific proofs that create the “normal science” environment. Kuhn, *Structure of Scientific Revolution*, 1.

110. There is a difference in a scientific hypothesis (untested but proposed explanation) versus a scientific theory (extensive testing is conducted and generally accepted as an accurate explanation). Richard Rumelt defines a scientific hypothesis as “a new idea or theory,” but this type of definition muddies the discussion, as a hypothesis and theory are not exactly synonymous (although dictionaries do show them as synonyms.) Rumelt, *Good Strategy/Bad Strategy*, 247. My interpretation is that a hypothesis is “a tentative assumption” before testing, whereas a theory is a “plausible or scientifically acceptable general principle or body of principles offered to explain phenomena.” In other words, a hypothesis is untested, and a theory has parameters to test against that are already accepted as norms. *Merriam-Webster’s Collegiate Dictionary*, 11th ed., s.v. “hypothesis.”

111. “The Air Force Targeting Roadmap provides the foundation to develop an action plan to revitalize Air Force targeting capability and ensure that the Air Force is organized, trained and equipped to support joint and coalition forces. This roadmap articulates Air Force senior leaders’ guidance to drive policy and resource decisions that achieve a robust, effective, and efficient Air Force targeting capability.” For more specifics, see Shwedo, “Air Force Targeting Roadmap,” 8.

112. The joint cyber forces train together in cyber ranges intended to validate “cyber technologies by emulating complex defense and commercial networks.” “National Cyber Range Completes Beta Phase.” Additionally, joint exercises that go beyond the virtual cyber ranges include activities such as Terminal Fury 2011. Exercises such as these enable operational testing of concepts like Adaptive Network Defense of Command and Control, which enables JFC control of key terrain in cyberspace. These are exactly the synchronized efforts cyber forces will require to confront the adaptive nature cyberspace affords adversaries who will choose to confront the United States in the newest war-fighting domain. For more on Terminal Fury, see Gonzalez, “Joint Experimentation Enables Regional Cyber Protection.”

113. There is already movement toward joint cyber training centers of excellence. The Cyber-City is one such example. The operation, which is run by a New Jersey-based security firm, is intended to provide soldier-hackers from the Air Force and other branches of the military with practice in attacking and defending computers and networks that run a theoretical town. Robert O’Harrow Jr., “CyberCity Allows Government Hackers to Train for Attacks,” *Washington Post*, 26 November 2012, http://articles.washingtonpost.com/2012-11-26/news/35508198_1_government-hackers-security-firm-digital-attacks.

114. *Live network* is sometimes the name given to the open Internet. If a training exercise goes bad, the effects are not felt by users of the public. These cyber ranges can be viewed as virtual simulator training like pilots use for training. This way if a plane crashes during simulator training, there is no physical damage or real-world costs.

115. See “The Quadrennial Review” in Betz and Stevens, *Cyberspace and the State*, 8.

116. Starr, “Toward a Preliminary Theory of Cyberpower,” 48.

117. See cybernetic warfare and computers and chaoplex warfare and the network in Bousquet, *Scientific Way of Warfare*, 33–34.

118. The Twenty-Fourth Air Force developed a “Weapons and Tactics Roadmap” in 2011 to help shape the development of an operational cyber force in regards to cyber warfare. Although the roadmap has not been approved/signed as of this writing, the Air Force has already moved forward with developing its cyber warriors. The first cyber weapons school class met in 2012 and developed both cadre and field tacticians alike. In addition to education and training, the Air Force cyber community has also developed a tiered list for outplacement of these highly skilled Airmen, which affords development and experience opportunities from the tactical through strategic levels. This effort is a great start in developing a required cadre of experts the Air Force must invest in for its future success in cyber war. See the unpublished draft of the Air Force Space Command, “Twenty-Fourth Air Force Weapons and Tactics Roadmap.”

119. Advocacy to gather critical strategic thinkers from all the key players in government and the private sector to advance thought in the new domain of cyberspace appeared in a recent *Air & Space Power Journal*. The authors proclaimed that standing up a “cyber” ACTS, similar to the Air Corps Tactical School for airpower during its infancy, would leverage talent resources from academia, research and development, and operational experience to cultivate ideas regarding cyberspace. Fadok and Raines, “Driving towards Success,” 4–11.

120. Sherry, *Rise of American Air Power*, 63.

121. Clausewitz, *On War*, 141.

122. *Ibid.*

Chapter 6

Conclusion

The acceptance or rejection of an invention, or to the extent to which its implications are realized if it is accepted, depends quite as much upon the condition of society, and upon the imagination of its leaders, as upon the nature of the technological item itself.

—Lynn White
Medieval Technology and Social Change

Maj Gen Suzanne Vautrinot, Air Forces cyber commander, argues that the Air Force can leverage cyberspace to create integrated effects to respond to crises and conduct uninterrupted operations.¹ I agree but recommend that the Air Force clearly define what cyberspace effects it desires to create so it is organizing, training, and equipping a cyber force ready to respond to tomorrow's crises. By publicly announcing that Air Force policy is to defend specific national security interests, as well as actively oppose cyber attacks with offensive cyber operations, cyberspace security surrounding military operations will increase while cyber force professionals gain invaluable experience. By defining and publicizing acceptable and unacceptable behaviors, international norms will no longer be left to arbitrary precedence. These actions will drive cyberspace standards within the US military, as well as acceptable US and international norms throughout cyberspace. If the United States chooses not to lead cybersecurity efforts, another nation will, and it may not be in the direction of US national interests. If this occurs, US cyberspace operations will become more reactive than they are today.

Evaluating the early theories of airpower advocates like Douhet, Trenchard, and Mitchell can aid cyber theorists. Understanding and identifying where cyber power can influence military operations and target adversary centers of gravity will shape US military efforts in achieving political objectives. However, given the infancy of cyberspace, along with the limited use of cyber power to influence conflict resolution, many military cyberspace operations are guided by hypothetical potential instead of tested results. It is applicable for the US Air Force to examine the theory and doctrine, as well as the tactics, techniques, and procedures ACTS evaluated throughout the 1920s and 1930s. Airpower targeting theories such as the industrial web theory guided Army Air Corps education and training objectives before World War II. It also shaped OT&E functions by focusing airpower efforts through the use of a

CONCLUSION

combined bomber offensive. Although these early theories are controversial to some, advocates focused on desired results and continued to learn what worked well and what did not. Continual evolution of technology eventually led airpower to become the force multiplier early advocates perceived it could be.

It can be argued that Operation Desert Storm was airpower's defining moment. The technology of airpower evolved to a point that precision bombing became a reality, and the speed and agility of which airpower could strike were realized. Airpower effectively destroyed the enemy's ability to operate as an effective fighting force by combining the system capabilities of airpower with Col John Warden's contemporary airpower theory. Colonel Warden suggests that cyber power theorists today can draw upon the doctrine, education, and training focus of ACTS and combine it with the strategic perspective of viewing the enemy as a system to develop an effective cyber-power targeting theory for use in future conflicts. There is little doubt that cyberspace will be employed before, during, and after all future wars in shaping the battleground, initiating a conflict, or going through all phases of military operations.

As military commanders evaluate the offensive, defensive, and exploitation roles that cyberspace affords, there are limitations that prevent a military's use of cyberspace from reaching its full potential. As civilian and military leaders grapple with challenges such as attribution or understanding centers of gravity that can be targeted by cyber power, a review of the required expertise and organization necessary to support cyberspace efforts may be required. As the United States seeks to protect its national security interests in, through, and from cyberspace activities, accepting cyberspace as a distinct domain has significant implications for equipping cyber forces and developing a culture for cyber activities.² These discussions may sound familiar to early airpower supporters who advocated a separate service before 1947 and thus are worth discussing in the fiscally strained environments of today, especially if duplication and inefficiencies are found across each service's efforts to wield cyber power.

Cyber power has not changed the nature of war, but it has changed the character. Military forces who want to be successful at winning future conflicts must embrace the potential affects and effects wielded by cyber power. Commanders must organize, train, and equip cyber forces to achieve desired results while limiting the ability of the adversary to do the same to friendly and allied force actions. Given the minimal lessons of cyber warfare that exists today, theorizing about cyber power effects and their cause is relevant. Although early theories may not lead to doctrinal principles that last through time, they will be an attempt at understanding the potential of cyber power. The choice to employ offense, defense, or exploitation as US cyber power's

primary role should not be arbitrary, something that appears to be the case across the international community today. If the United States defines what constitutes cyber war and cyber warfare and then defines acceptable and unacceptable behaviors, international norms throughout cyberspace will be shaped. It seems prudent to shape these efforts today rather than allowing the international community to dictate norms that do not protect US national security interests.

My intent is to espouse a cyber-power targeting theory, along with initial propositions of cyber power, to continue the dialog regarding US cyber power. Learning lessons from the evolution of airpower may not only shape how US military forces employ cyber power tomorrow, but may also save the nation's treasure by preventing mistakes similar to those of the past. If critical thinking surrounding cyberspace efforts enhances the OT&E endeavors of military forces, then militaries and policy makers are serving national interests accordingly.

Finally, American vulnerabilities to adversary actions in, through, or from cyberspace should become evident when we think about the true potential of cyber power. When this occurs, gaps can be closed, and confidence in future cyberspace operations and security should increase. The vulnerabilities of democracies to cyber attack are real, given society's current and continued reliance on cyberspace, especially in the United States. Therefore, it is critical to continually evaluate the cyber power of both the United States and its allies—and that of potential adversaries—if the nation truly intends to protect its national interests.

Notes

1. Vautrinot, "Sharing the Cyber Journey," 80.
2. Kramer, Starr, and Wentz, *Cyberpower and National Security*, 48.

Abbreviations

ACTS	Air Corps Tactical School
AFDD	Air Force doctrine document
AFIT	Air Force Institute of Technology
AFI	Air Force instruction
AFHRA	Air Force Historical Research Agency
AFSPC	Air Force Space Command
AWPD	air war planning document
C2	command and control
C-ACTS	Cyber Air Corps Tactical School
CENTCOM	Central Command
CNE	computer network exploitation
COMAFFOR	commander, Air Force Forces
CSAF	chief of staff of the Air Force
DCO	defensive cyber operations
DDOS	distributed denial of service
DOD	Department of Defense
DOE	Department of Energy
IADS	integrated air defense system
ICRC	International Committee of the Red Cross
ICJ	International Court of Justice
JFACC	joint force air component commander
JFC	joint force commander
JOA	joint operating area
JP	joint publication
LOC	lines of communication
MAD	mutual assured destruction
MAJCOM	major command
MCDP	Marine Corps doctrinal publication
NII	national information infrastructure
OCO	offensive cyber operations
ODNI	Office of the Director of National Intelligence
OODA	observe-orient-decide-act

ABBREVIATIONS

OT&E	organize, train, and equip
RAF	Royal Air Force
RFC	Royal Flying Corps
SAASS	School of Advanced Air and Space Studies
SCADA	supervisory control and data acquisition
TR	training regulation
UN	United Nations
USAF	US Air Force
USC	<i>United States Code</i>
USCYBERCOM	US Cyber Command
WTO	World Trade Organization

Bibliography

- Air Force Doctrine Document 1. *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011.
- Air Force Doctrine Document 3-12. *Cyberspace Operations*, Change 1, 30 November 2011.
- Air Force Doctrine Document 3-60. *Targeting*, Change 1, 28 July 2011.
- Air Force Historical Research Center (AFHRC). "Signal Corps Specification, No. 486." File 167.6-1, IRIS 1012791 (1907–1940). AFHRC, Maxwell AFB, AL.
- Air Force Instruction 14-117. *Intelligence: Air Force Targeting*, 13 May 2009.
- Air Force Space Command. "Twenty-Fourth Air Force Weapons and Tactics Roadmap." Draft Memo, 2011.
- Air War Plans Division (AWPD) 1. *Targeting for Victory*, 1941. <http://www.au.af.mil/au/awc/awcgate/readings/awpd-1-jfacc/awpdproc.htm>.
- Air War Plans Division 42. *Requirements for Air Ascendancy*, 1942. File 145.82-42. Air Force Historical Research Agency (AFHRA), Maxwell AFB, AL.
- Air War Plans Division 42. Pt. 4, "Report," 1942. File 145.82-42. Air Force Historical Research Agency (AFHRA), Maxwell AFB, AL.
- . Tab B-1-a, "Air Offensive—Europe," File 145.82-42. AFHRA, Maxwell AFB, AL.
- Amoroso, Edward. *Cyber Attacks: Protecting National Infrastructure*. Kidlington, Oxfordshire (UK): Elsevier Science, 2010.
- Anderson, Maj Gen Orville. "Air Warfare and Morality." *Air University Quarterly Review* 2 (Winter 1949): 7.
- Arnold, Gen Henry. To the chief of staff. Memorandum, pt. 2. Subject: Combat Aircraft Which Should Be Produced in the United States in 1943, 9 September 1942.
- . To the chief of staff. Memorandum. Subject: Answering Memo and Outline of Report. In AWPD 42. File 145.82-42. AFHRA, Maxwell AFB, AL.
- Barlow, Jeffrey G. *The Revolt of the Admirals: The Fight for Naval Aviation, 1945-50*. Washington, DC: Ross & Perry Inc., 2001.
- Belote, Maj Howard. "Warden and the Air Corps Tactical School: What Goes Around Comes Around." *Airpower Journal* 13, no. 3 (Fall 1999). <http://www.airpower.au.af.mil/airchronicles/apj/apj99/fal99/belote.html>.
- Betz, David J., and Timothy C. Stevens. *Cyberspace and the State: Toward a Strategy for Cyberpower*. New York: Taylor & Francis Group, 2012.
- Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945*. Princeton, NJ: Princeton University Press, 2004.

BIBLIOGRAPHY

- Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battle Fields of Modernity*. New York: Columbia University Press, 2010.
- Bowden, Mark. *Worm: The First Digital World War*. New York: Grove/Atlantic, 2011.
- Boyd, Col John, USAF, retired. Compendium. "The Essence of Winning and Losing." Project on Government Oversight, Defense and the National Interest, August 2010. <http://dnipogo.org/?s=essence+of+winning+and+losing>.
- Boyko, Alexander, Sergey Popov, and Nemanja Krasjistik. "Investigating the Sayano-Shushenskaya Hydro Power Plant Disaster." *Power*, 1 December 2010. <http://www.powermag.com/investigating-the-sayano-shushenskaya-hydro-power-plant-disaster/>.
- Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.
- Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York: Oxford University Press, 2009.
- Brodie, Bernard. "The Morale Factor in STRAP Planning," 5 August 1949. Box 11, Folder 17, Papers of Bernard Brodie. Los Angeles: University Research Library, Special Collections Division, University of California at Los Angeles.
- . *Strategy in the Missile Age: Theory and Applications*. Lanhan, MD: National Book Network, 2007.
- Bumgarner, John. "Computers as Weapons of War." *IO Journal* (May 2010). <http://www.nxtbook.com/nxtbooks/naylor/JEDQ0210/index.php?startid=4#/4>.
- Calhoun, Martin. *US Military Spending, 1945–1991*. Report. Washington, DC: Center for Defense Information, 9 July 1996. <http://academic.brooklyn.cuny.edu/history/johnson/milspend.htm>.
- Carroll, Lewis. *Alice's Adventures in Wonderland*. New York: Macmillan, 1869.
- Case Concerning the Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*. International Court of Justice (ICJ), 27 June 1986. ICJ Section X 2. <http://www.icj-cij.org/docket/?sum=367&code=nus&p1=3&p2=3&case=70&k=66&p3=5>.
- Center for Global Development. *Phase Zero: The Pentagon's Latest Big Idea*. Report. Washington, DC: Center for Global Development, 20 July 2007. <http://www.cgdev.org/blog/phase-zero-the-pentagons-latest-big-idea>.
- Charter of the United Nations. Chap. 1, art. 2, sec. 4. (<http://www.un.org/en/documents/charter/chapter1.shtml>).
- . Chap. 7, art. 39. <http://www.un.org/en/documents/charter/chapter7.shtml>.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins Publishers, 2010.

- Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.
- Clodfelter, Mark. *The Limits of Airpower: The American Bombing of North Vietnam*. Lincoln: University of Nebraska Press, 2006.
- Cody, James R. "AWPD-42 to Instant Thunder." Master's thesis, School of Advanced Airpower Studies, June 1996.
- Conference Report on H. R. 1540, *National Defense Authorization Act for Fiscal Year 2012*. Sec. 954, "Military Activities in Cyberspace." *Congressional Record* 157, no. 190, 12 December 2011. http://www.fas.org/irp/congress/2011_cr/cyberwar.html.
- Craig, Cambell. *Destroying the Village: The Prospect of Thermonuclear War in American Security Policy*. New York: Columbia University Press, 1998.
- Crane, Conrad C. *American Airpower Strategy in Korea, 1950-1953*. Lawrence: University Press of Kansas, 2000.
- Department of Defense. Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 (Washington, DC: DOD, November 2011).
- . *DOD Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, July 2011.
- De Seversky, Alexander P. *Victory through Air Power*. New York: Simon and Schuster, 1942.
- Dolman, Everett C. *Astropolitik: Classical Geopolitics in the Space Age*. London: Taylor & Francis, 2001.
- Donnelly, John. "Cohen: Attack on US Satellite Is Attack on United States." *Defense Week*, 26 July 1999.
- Douhet, Giulio. *The Command of the Air*. Edited by Joseph P. Harahan and Richard H. Kohn. Translated by Dino Ferrari. Tuscaloosa: University of Alabama Press, 2009.
- Dunlap, Charles. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 81-99.
- Faber, Lt Col Peter. "Competing Theories of Airpower: A Language for Analysis." Paper presented at the Aerospace Power Doctrine Symposium. Maxwell AFB, AL, 30 April 1996.
- Fadok, Lt Gen David, and Dr. Richard Raines. "Driving towards Success in the Air Force Cyber Mission." *Air & Space Power Journal* 26, no. 5 (September-October 2012): 4-11.
- Ferrill, Arther. *The Origins of War: From the Stone Age to Alexander the Great*. Boulder, CO: Westview Press, 1997.
- Finney, Robert T. *History of the Air Corps Tactical School, 1920-1940*. Washington, DC: Center for Air Force History, 1955.

BIBLIOGRAPHY

- Fischer, Eric. "Federal Law Relating to Cybersecurity: Discussion of Proposed Revisions." *Congressional Research Service Report for Congress*, 9 November 2012. <http://www.fas.org/sgp/crs/natsec/R42114.pdf>.
- Forsyth, James Wood Jr. "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly* 7, no.1 (Spring 2013): 93–113.
- Foulois, Maj Gen Benjamin. Transcript of oral history interview, 9 December 1965. K239.0512-766. AFHRC, Maxwell AFB, AL.
- Futrell, Robert F. *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force*. Darby, PA: Diane Publishing, 1971.
- . *Ideas, Concepts, Doctrine*. Vol. 2, *Basic Thinking in the United States Air Force 1961–1984*. Maxwell AFB, AL: Air University Press, 1989.
- Glock, Capt John. "The Evolution of Air Force Targeting." *Airpower Journal* 8, no. 3 (Fall 1994): 14–28.
- Goldstein, Frank L., and Benjamin F. Findley. *Psychological Operations: Principles and Case Studies*. Maxwell AFB, AL: Air University Press, 1996.
- Gonzalez, Jose. "Joint Experimentation Enables Regional Cyber Protection." *Signal*, 1 February 2013.
- Gray, Colin, "The Airpower Advantage in Future Warfare: The Need for Strategy." Research paper 2007–2. Maxwell AFB, AL: Air Force Doctrine and Development Education Center, December 2007.
- Gray, Colin S., *Airpower for Strategic Effect*. Maxwell AFB, AL: Air University Press, 2012.
- Gross, Michael Joseph. "A Declaration of Cyber-War." *Vanity Fair*, April 2011. <http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104>.
- Grossman, Dave, and Loren W. Christensen. *On Combat: The Psychology and Physiology of Deadly Conflict in War and Peace*. Belleville, IL: PPCT Research Publications, 2007.
- Hadnagy, Christopher, and Paul Wilson. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley, 2010.
- Hallion, Richard. *Storm over Iraq: Airpower and the Gulf War*. Smithsonian Institution Press, 1992.
- . *Storm over Iraq Pb*. Washington, DC: Smithsonian, 1997.
- Hansell, Haywood S. *The Air Plan That Defeated Hitler*. Atlanta, GA: Arno Press, 1980.
- Hart, Gary. "After bin Laden: Security Strategy and the Global Commons." *Survival: Global Politics and Strategy* 53, no.4 (August–September 2011): 19–25.
- Hoig, Stan, Paul Rosier, and Ada E. Deer. *The Cheyenne*. New York: Facts On File, Incorporated, 2009.

- Hurley, Alfred F. *Billy Mitchell, Crusader for Airpower*. Bloomington: Indiana University Press, 1975.
- Hurley, Matthew. "For and From Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance." *Air & Space Power Journal* 26, no. 6 (November–December 2012): 12–33 <http://www.airpower.au.af.mil/digital/pdf/articles/Nov-Dec-2012/F-Hurley.pdf>.
- Hurwitz, Roger. "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly* 6, no.3 (Fall 2012): 20–45.
- International Committee of the Red Cross. *Declaration (IV, 1), to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons, and Other Methods of Similar Nature*. The Hague, 29 July 1899. <http://www.icrc.org/applic/ihl/ihl.nsf/INTRO/160?OpenDocument>.
- . *Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons*. International Peace Conference at The Hague, 18 October 1907. <http://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=10BB640A9FF13B49C12563CD002D6895>.
- Jabbour, Dr. Kamal. "The Science and Technology of Cyber Operations." *High Frontier* 5, no. 3 (May 2009): 11–15. <http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf>.
- Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 15 March 2013.
- Joint Publication 3-0. *Joint Operations*, 11 August 2011.
- Joint Publication 3-12. *Cyberspace Operations*, 5 February 2013.
- Joint Publication 3-60. *Joint Targeting*, 13 April 2007.
- Joint Publication 5-0. *Joint Operation Planning*, 11 August 2011.
- Joynton-Hicks, William. *The Command of the Air; or, Prophecies Fulfilled; Being Speeches Delivered in the House of Commons*. London: Nisbet, 1916.
- Kainikara, Sanu, and RAAF Airpower Development Centre. *Principles of War and Airpower*. Canberra, Australia: Airpower Development Centre, 2011.
- Kalyvas, Stathis N. *The Logic of Violence in Civil War*. New York: Cambridge University Press, 2006.
- Keaney, Thomas A., Eliot Cohen, and Gulf War Air Power Survey Review Committee. *Gulf War Air Power Survey*. Vol. II, *Operations and Effects and Effectiveness*. Washington, DC: US Department of Defense, 1993.
- Keaney, Thomas A., and Eliot Cohen. *Gulf War Air Power Survey: Summary Report*. Washington, DC: US Government Printing Office, 1993.
- Kennett, Lee B. *The First Air War: 1914–1918*. New York: Simon & Schuster, 1999.
- Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: Potomac Books Incorporated, 2009.

BIBLIOGRAPHY

- Krekel, Bryan A., Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. US–China Economic and Security Review Commission Report. Washington, DC: CreateSpace Independent Publishing Platform, 2012.
- Kuhn, Thomas S. *The Structure of Scientific Revolutions*. 3rd ed. Chicago: University of Chicago Press, 1996.
- Libicki, Martin. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.
- . “The Specter of Non-Obvious Warfare.” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 88–101.
- Lin, Patrick, Fritz Allhoff, and Neil Rowe. “Is It Possible to Wage a Just Cyberwar?” *The Atlantic*, 5 June 2012. <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106>.
- Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York: Frank Cass, 2004.
- Lynn, William. “The Pentagon’s Cyberstrategy: One Year Later.” *Foreign Affairs*, 28 September 2011.
- Manifold, Maj Chad. “Project Air Force Project Description Improving Air Force Target Intelligence.” Maxwell AFB, AL: School of Advanced Air and Space Studies, November 2012.
- Marine Corps Document Publication 1. *Warfighting*, 20 June 1997.
- Maurer, Tim. *Cyber Norm Emergence at the United Nations*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. <http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf>.
- McDougall, Walter A. *The Heavens and the Earth: A Political History of the Space Age*. Baltimore, MD: Johns Hopkins University Press, 1997.
- Meilinger, Phillip S. “Ten Propositions Regarding Airpower.” *Airpower Journal* 7, no. 2 (Summer 1993).
- Miller, Roger G. *To Save a City: The Berlin Airlift, 1948–1949*. College Station: Texas A&M University Press, 2008.
- Mitchell, William. *Winged Defense*. Port Washington, NY: Associated Faculty Press Inc, 1925.
- Mitchell, William, and Robert S. Ehlers. *Winged Defense: The Development and Possibilities of Modern Airpower—Economic and Military*. Tuscaloosa: University of Alabama Press, 2010.
- Moltke, Helmuth. *Moltke on the Art of War: Selected Writings*. Edited and translated by Daniel J. Hughes. New York: Random House Publishing Group, 1995.

- Momyer, William W. *Airpower in Three Wars*. Washington, DC: Department of the Air Force, 1978.
- Morgan, Forrest E. *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*. Santa Monica, CA: RAND Corporation, 2010.
- Morocco, John D. "From Vietnam to Desert Storm," *Air Force Magazine* 5, no. 1 (January 1992): 68–73. <http://www.airforcemag.com/MagazineArchive/Pages/1992/January%201992/0192storm.aspx>.
- Mowbray, James A. "Air Force Doctrine Problems: 1926–Present." *Airpower Journal* 9, no. 4 (Winter 1995): 2–17.
- Napolitano, Janet, secretary of the Department of Homeland Security. "Remarks by Secretary Napolitano before the Joint Meeting of the OSCE Permanent Council and ASCE Forum for Security Cooperation." Department of Homeland Security news release, 1 July 2011. <http://www.dhs.gov/news/2011/07/01/remarks-secretary-napolitano-joint-meeting-osce-permanent-council-and-osce-forum>.
- "National Cyber Range Completes Beta Phase." *Air Force Magazine*, 21 November 2012. <http://www.airforcemag.com/DRArchive/Pages/2012/November%202012/November%2021%202012/NationalCyberRangeCompletesBetaPhase.aspx>.
- National Security Strategy*. Washington, DC: White House, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
- National Security Strategies. Washington, DC: National Security Archives, May 2010. <http://nssarchive.us/>.
- National Space Policy of the United States of America*. Washington, DC: Executive Office of the President, 28 June 2010.
- Office of the Director of National Intelligence. *The IC and Cyberspace: Traditions, Boundaries, and Governance*. Washington, DC: National Intelligence Agency, August 2010.
- Olsen, John A. *John Warden and the Renaissance of American Airpower*. Dulles, VA: Potomac Books Incorporated, 2007.
- Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, MA: Harvard University Press, 1965.
- "Opening of Hostilities (Hague III)." *Hague Convention of 1907*. http://avalon.law.yale.edu/20th_century/hague03.asp.
- Osinga, Frans P. B. *Science, Strategy and War: The Strategic Theory of John Boyd*. New York: Taylor & Francis, 2007.
- Pape, Robert A. *Bombing to Win: Airpower and Coercion in War*. Ithaca, NY: Cornell University Press, 1996.

BIBLIOGRAPHY

- Paret, Peter, Gordon A. Craig, and Felix Gilbert. *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Princeton, NJ: Princeton University Press, 2008.
- Peattie, Mark R. *Sunburst: The Rise of Japanese Naval Airpower, 1909–1941*. Annapolis, MD: Naval Institute Press, 2007.
- Pfaltzgraff, Robert Jr., and Richard H. Shultz, Jr., eds. *Future of Airpower in the Aftermath of the Gulf War*. Maxwell AFB, AL: Air University Press, 1992.
- Ponemon Institute. “Second Annual Cost of Cyber Crime Study.” Benchmark Study of US Companies. Traverse City, MI: Ponemon Institute, August 2011. http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.
- Putney, Diane T. “From Instant Thunder to Desert Storm: Developing the Gulf War Air Campaign’s Phases.” *Air Power History* 41, no. 3 (Fall 1994): 38–50.
- Raleigh, Walter A., and H. A. Jones. *The War in the Air: Being the Story of the Part Played in the Great War by the Royal Air Force*. Oxford, UK: Clarendon Press, 1922.
- Randolph, Stephen P. *Powerful and Brutal Weapons: Nixon, Kissinger, and the Easter Offensive*. Cambridge, MA: Harvard University Press, 2007.
- Reed, John. “The Pentagon is Tweaking the Cyber Capabilities It Wants from the Services.” *Foreign Policy*, 30 November 2012. http://killerapps.foreignpolicy.com/posts/2012/11/30/the_pentagon_is_tweaking_the_cyber_capabilites_it_wants_from_the_services.
- Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.
- Rid, Thomas. “Cyber Fail: The Obama Administration’s Lousy Record on Cyber Security.” *New Republic*, 4 February 2013. <http://www.newrepublic.com/article/112314/obama-administrations-louse-record-cyber-security>.
- . “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32.
- Rueschhoff, Jan, and Jonathan Dunne. “Centers of Gravity from the ‘Inside Out.’” *Joint Forces Quarterly* 60, no. 1 (1st Quarter 2011): 120–25. <http://www.ndu.edu/press/jfq-60.html>.
- Rumelt, Richard. *Good Strategy/Bad Strategy: The Difference and Why It Matters*. New York: Crown Publishing Group, 2011.
- Sample, Timothy. “Calling for a National-Level Doctrine for the Cyber Era.” *Defense Systems*, 18 December 2012. <http://defensesystems.com/Articles/2012/12/18/special-commentary-cyber-era-doctrine.aspx?p=1>.
- Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.

- Schmitt, Eric, and Thom Shanker. *Counterstrike: The Untold Story of America's Secret Campaign against Al Qaeda*. New York: Henry Holt and Company, 2011.
- Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.
- Segal, Adam, Maurice Greenberg, and Matthew Waxman. "Why a Cybersecurity Treaty Is a Pipe Dream." *Council on Foreign Relations*, 27 October 2011. <http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325>.
- Sheldon, John B. "State of the Art: Attackers and Targets in Cyberspace." *Journal of Military and Strategic Studies* 14, no. 2 (2012): 6–11.
- Sherry, Michael S. *The Rise of American Airpower: The Creation of Armageddon*. New Haven, CT: Yale University Press, 1987.
- Shiner, John P. *J.S.S. Foulois and the U.S. Army Air Corps: 1931–1935*. Washington DC: Diane Publishing, 1983.
- Shwedo, Brig Gen Bradford, director of intelligence, Air Combat Command. "Air Force Targeting Roadmap: Reinvigorating Air Force Targeting." Draft Article, 30 September 2012.
- Steiner, Barry H. *Bernard Brodie, and the Foundations of American Nuclear Strategy*. Lawrence: University Press of Kansas, 1991.
- Strange, Joe, and Richard Iron. "Understanding Centers of Gravity and Critical Vulnerabilities: Part 1." <http://www.au.af.mil/au/awc/awcgate/usmc/cog1.pdf>.
- Strassler, Robert B., and Victor D. Hanson. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. New York: Simon & Schuster, 1998.
- Suffolk, John. "Cyber Security Perspectives." *Huawei*, September 2012. http://www.huawei.com/ilink/en/download/HW_187368.
- Sun Tzu. *The Illustrated Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 2005.
- Tanaka, Yuki, and Marilyn B. Young. *Bombing Civilians: A Twentieth-Century History*. New York: New Press, 2010.
- Title 50, War and National Defense. *US Code*, sec. 932, 4 January 2012. http://www.law.cornell.edu/uscode/pdf/lii_usc_TI_50.pdf. This section was repealed on 10 August 1956.
- Tooze, Adam. *The Wages of Destruction: The Making and Breaking of the Nazi Economy*. New York: Penguin Books, 2008.
- Tyson, Neil G., and Avis Lang, ed. *Space Chronicles: Facing the Ultimate Frontier*. New York: W. W. Norton, 2012.
- USAF Historical Research Library. "Development of the U.S. Air Forces Philosophy of Air Warfare Prior to Our Entry into World War II." MICFILM 34142, Jan 1 1929–Jan 1 1964, Series 3, Box 4, Folder 1, Speech 5. Historical Research Library, Maxwell AFB, AL.

BIBLIOGRAPHY

- US Air Force. "2013 Air Force Mission Statement," 2013. <http://www.posturestatement.af.mil/main/welcome.asp>.
- US House. *2013 National Defense Authorization Act*. 112th Cong., 2nd sess., 3 January 2012. <http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf>.
- . *Department of the Air Force Presentation to the Committee on Armed Services, United States House of Representatives: Fiscal Year 2013 Air Force Posture Statement of the Honorable Michael B. Donley, Secretary of the Air Force, and General Norton A. Schwartz, Chief of Staff, United States Air Force*. 112th Cong., 2nd sess., 28 February 2012. <http://www.posturestatement.af.mil/shared/media/document/AFD-120321-055.pdf>.
- Valeri, Lorenzo. "Countering Threats in Space and Cyberspace: A Proposed Combined Approach." International Security Discussion Paper. London: Chatham House, January 2013. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0113discussionpaper_Valeri.pdf.
- Vautrinot, Maj Gen Suzanne. "Sharing the Cyber Journey." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 71–87.
- Wakelam, Randall Thomas. *The Science of Bombing: Operational Research in RAF Bomber Command*. Toronto: University of Toronto Press, 2009.
- Walt, Stephen M. "Kenneth N. Waltz, 1924–2013." *Foreign Policy*, 13 May 2013. <http://foreignpolicy.com/2013/05/13/kenneth-n-waltz-1924-2013/>.
- Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press, 2001.
- . *Theory of International Politics*. Long Grove, IL: Waveland Press Inc., 2010.
- Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York: Basic Books, 2006.
- Warden, John A. III. *The Air Campaign: Planning for Combat*. Bloomington, IN: iUniverse, 2000.
- Watts, Barry D. *The Foundations of US Air Doctrine: The Problem of Friction in War*. Maxwell AFB, AL: Air University Press, 1984.
- Waxman, Matthew. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36, no.2 (Fall 2010): 421–59. <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf>.
- Welch, Gen Larry. "Cyberspace—The Fifth Operational Domain." *IDA Research Notes—Challenges in Cyberspace*, Summer 2011. <https://www.ida.org/upload/research%20notes/researchnotessummer2011.pdf>.
- Wells, H. G. *The War in the Air*. New York: Boni and Liveright, Incorporated, 1917.

- Welsh, Gen Mark A. III. "Speech to the Air Force Association Air & Space Conference and Technology Exposition." Speech. Air Force Association Air & Space Conference, National Harbor, MD, 18 September 2012. <http://www.af.mil/Portals/1/documents/csaf/air-space-conference-2012.pdf>.
- . "A Vision for the United States Air Force." 2013 Air Force Mission Statement. <http://www.posturestatement.af.mil/main/welcome.asp>.
- White, Lynn Jr. *Medieval Technology & Social Change*. Oxford, UK: Oxford University Press, 1964.
- Williams, Brig Gen Brett. "Ten Propositions Regarding Cyberspace Operations." *Joint Forces Quarterly* 61 (2nd Quarter 2011): 10–17.
- Winton, Harold. "An Imperfect Jewel: Military Theory and the Military Profession." *Journal of Strategic Studies* 34, no. 6 (December 2011): 853–77.
- Worldometers. "Current World Population." <http://www.worldometers.info/world-population/>.
- Zhang, Xiaoming. *Red Wings over the Yalu: China, the Soviet Union, and the Air War in Korea*. College Station: Texas A&M University Press, 2003.
- Zhengde, Wang, Yang Shisong and Zhou Lin, eds. *Xinxi Duikang Lilun (Information Confrontation Theory)*. Beijing: PLA Information Engineering University/ Military Science Publishing House, 2007.



AFRI **AIR PRESS**
AIR FORCE RESEARCH INSTITUTE

ISBN: 978-1-58566-238-8

ISSN: 1941-3785